内容中心网络安全技术研究综述

朱大立[1,2], 梁 杰[1,2], 李 婷[1,2], 张杭生[1,2], 耿立茹[1], 吴 荻[1],
张天魁[3], 刘银龙[1,2]

[1] 中国科学院信息工程研究所 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049
[3] 北京邮电大学网络体系构建与融合北京市重点实验室 北京 中国 100876

摘要 内容中心网络(Content Centric Networking, CCN)属于信息中心网络的一种, 是未来互联网体系架构中极具前景的架构之一, 已成为下一代互联网体系的研究热点。内容中心网络中的内容路由、内嵌缓存、接收端驱动传输等新特征, 一方面提高了网络中的内容分发效率, 另一方面也带来了新的安全挑战。本文在分析 CCN 工作原理的基础上, 介绍了 CCN 的安全威胁、安全需求以及现有的解决方案, 并展望了 CCN 安全技术研究的方向。首先, 详细介绍了 CCN 的原理和工作流程, 对比分析了 CCN 与 TCP/IP 网络的区别, 并分析了 CCN 面临的安全威胁及需求。其次, 对 CCN 中隐私保护、泛洪攻击、缓存污染、拥塞控制等技术的研究现状进行归纳、分析、总结, 并分析了现有方案的优缺点及不足, 进而分析可能的解决方案。最后, 对 CCN 安全技术面临的挑战进行了分析与讨论, 并展望了未来的研究方向及发展趋势。通过对已有研究工作进行总结与分析, 本文提出了 CCN 安全技术潜在研究方向与关键问题, 为 CCN 安全后续研究提供有益参考。

关键词 内容中心网络; 安全; 访问控制; 隐私保护; 泛洪攻击; 缓存污染; DoS; 网络拥塞
中图法分类号 TP393 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2020.09.09

A Survey of Security in Content Centric Networking

ZHU Dali[1,2], LIANG Jie[1,2], LI Ting[1,2], ZHANG Hangsheng[1,2], GENG Liru[1], WU Di[1],
ZHANG Tiankui[3], LIU Yinlong[1,2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3]Beijing Key Laboratory of Network System Architecture and Convergence, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract Content Centric Networking (CCN) belongs to the Information Centric Networking (ICN) and is one of the most promising architectures in the future Internet architecture system. It has become a research hotspot of the next generation Internet system. The new features of CCN, such as content routing, in-network caching, and receiver-driven transmission can improve the content distribution efficiency in the network. However, it also can bring new security challenges. In this paper, we introduce CCN security threats, security requirements and existing solutions, and look forward to the possible direction of CCN security technology research based on the analysis of the working principle of CCN. Firstly, the operating principle and workflow of CCN are introduced in detail. The differences between CCN and TCP/IP are compared and analyzed, and the security threats and security requirements of CCN are analyzed. Secondly, the research status of privacy protection, flooding attack, cache pollution, network congestion and other technologies in CCN are summarized and analyzed, and analyzed the advantages and shortcomings of existing solutions and then analyzes possible solutions. Finally, the challenges faced by CCN security technology are analyzed and discussed and then we look forward to the future research direction and development trend. By summarizing and analyzing existing research work, we propose potential research directions and key issues, which can provide a useful reference for further study of CCN security.

Key words content centric networking; security; access control; privacy preserving; flooding attack; cache pollution attack; Dos attack; network congestion

1 概述

互联网创建之初主要是为了实现主机之间端到端的数据传输, 网络中的每个主机拥有一个全球唯一的 IP 地址, 通信源节点获取到目的节点 IP 之后在两个节点之间建立一条通信链路进行通信。近年来,

通讯作者: 刘银龙, 博士, 副研究员, Email: liuyinlong@iie.ac.cn。
本课题得到国家自然科学基金(No. 61303251); 北京市科技重大专项(No. D181100000618002)资助。
收稿日期: 2018-08-21; 修改日期: 2019-01-02; 定稿日期: 2020-08-24

随着互联网用户数量的增加、网络规模的扩大以及业务类型的多样化, 网络中的数据类型和通信模式发生了巨大变化, 网络中的流量主体不再是端到端通信, 而是数量巨大的内容分发。Cisco 视觉网络指数(Visual Networking Index, VNI)指出, 到 2020 年, 全球互联网流量将达到 2005 年全球互联网流量的 95 倍, 其中视频流量将占所有互联网流量的 82%[1], 这些视频流量的内容分发需要耗费大量的网络资源, 这给互联网服务提供商(Internet Service Provider, ISP)带来了巨大的压力。

针对 IP 网络中的内容分发问题, 研究人员做出了很多努力, 提出了采取内容分发网络(Content Delivery Network, CDN)、点对点(Peer to Peer, P2P)网络或 CDN 与 P2P 结合的技术来缓解网络中的内容分发压力。这些技术虽然能在一定程度上缓解网络压力, 但是这些方法都是在 IP 网络基础上的改良方案, 并不能从根本上解决 IP 网络存在的内容分发效率低下的问题。另外, IP 网络还存在四个固有的难以解决的问题: 地址空间耗尽、网络地址转换(Network Address Translation, NAT)遍历、移动性和地址管理[2]。与此同时, 对于网络中绝大部分的网络流量, 用户不再关心内容位置, 而只关注内容本身。从而, 促使国内外科研工作者探索更具可扩展性的互联网设计, 以实现高效的内容分发。

在此背景下, 信息中心网络(Information-Centric Networking, ICN)[3]应运而生, 逐渐成为未来网络领域的研究热点, 并已于 2017 年 5 月被国际电信联盟(International Telecommunication Union, ITU)列入 5G 的研究标准, 以期实现 5G 环境下的超低延迟通信。ICN 将当前以主机为中心的范式(即, 所有内容请求都发送到由 IP 地址标识的主机)转变为以信息为中心的范式(即, 将命名内容对象与它们所在的主机分离), 当前, 比较具有代表性的 ICN 架构包括 DONA(Data-Oriented Network Architecture)[4] 、CCN(Content-Centric Networking)[5] 、NDN(Named Data Networking)[6]、PSIRP(Publish Subscribe Internet Routing Paradigm)[7] 、PURSUIT(Publish Subscribe Internet Technology)[8]、NetInf(Network of Information)[9]和 Mobility First[10]。其中, CCN 和 NDN 是最典型也是被科研人员研究最多的 ICN 架构。

内容中心网络(Content Centric Networking, CCN)[5]由 Palo Alto 研究中心在 2009 年提出, 已成为未来网络最有发展潜力的网络架构之一。在内容中心网络体系结构中, 内容是网络的核心, 用户使用内容名字来请求内容。与现存的 IP 网络中的 DNS 类似, CCN 采用分层命名的方式, 网络中用内容名称进行路由, 类似于 IP 网络中基于前缀的路由。CCN 支持多源传输, 内容传输过程中允许被缓存在网络中的任何节点上, 所有缓存内容的节点均可为网络中的其他用户提供服务。2010 年, 命名数据网络(Named Data Networking, NDN)[7]遵循相同的设计原则, 被美国国家科学基金会(National Science Foundation, NSF)选中作为 NSF 未来互联网架构计划资助的四个项目之一。研究表明, CCN 和 NDN 仅是叫法不同, 并无本质上的区别, 因此下文对 CCN 和 NDN 不作区分。近几年, 我国国家自然科学基金和国家科技重大专项也相继资助了很多项目来对 CCN 进行研究, 如“内容中心车联网容量分析与缓存优化研究”、“内容中心移动社交网络高效安全匿名通信机制研究”、“基于社交关系与软件定义的内容中心网络多路转发及缓存机制研究”等等。

CCN 网络架构通过采取网内缓存(in-network caching)、多源传输等措施能够有效提高内容分发效率, 并且通过采用内容名称路由的方式可以消除一些传统网络中的安全问题(如多数传统形式的拒绝服务(Denial of Service, DoS)攻击)。尽管如此, 由于 CCN 属于开放式的网络架构且具有网内缓存和内容路由等独有特点, 许多专门针对 CCN 的新型网络攻击相继出现。研究发现, CCN 面临的安全问题主要有: 用户隐私泄露、兴趣包泛洪、缓存污染和网络拥塞, 其中兴趣包泛洪和缓存污染是由 DoS 攻击引发的安全问题。

当前学术界对 CCN 的研究工作主要集中在内容缓存、内容路由等提高网络中的内容分发效率的方向, 对于 CCN 中安全问题的综述性研究较少。鉴于安全技术在 CCN 中占据非常重要的地位, 且目前该技术的分类总结工作较少, 本文试图对 CCN 中的安全问题进行分类, 并对每一类安全问题的研究内容、研究现状及未来可能的发展方向进行综述, 具体贡献如下:

(1) 对 CCN 安全问题进行重新分类, 重点分析隐私泄露、DoS 攻击、网络拥塞三大安全问题; (2)从最新的参考文献出发, 系统地介绍了这些安全问题的最新研究进展, 分析了现有研究成果存在的问题并提出了未来的发展趋势; (3)探讨了 CCN 安全领域目前的热点问题, 并预测下一步的研究方向。

本文第二节主要阐述了 CCN 的基本原理, 并对 CCN 中的安全需求进行分类、总结。第三、四、五节分别分析了 CCN 中隐私保护、DoS 攻击和拥塞控制三个安全问题的研究现状及存在问题, 并预测未

来可能应用的技术。第六节指出了 CCN 安全技术研究的未来发展方向, 并总结全文。

2 CCN 及其安全需求

借助于内容名称路由、网内缓存、多源传输、多径路由等技术, CCN 能够解决传统 IP 体系结构在内容共享方面存在的许多不足。一方面, CCN 采用内容与位置分离的设计原则, 利用基于命名的路由方式, 使通信不再依赖源节点与目的节点之间的端到端连接, 能够更好地支持网络节点移动性。另一方面, CCN 采用网内缓存技术, 中间节点可以缓存经过该节点的数据, 为后续的内容请求直接提供服务, 减少用户请求响应时间并降低重复传输产生的网络流量, 提高了网络的鲁棒性。

本节首先介绍 CCN 的基本原理和工作流程, 并在此基础上分析 CCN 的主要特点, 最后介绍 CCN 面临的安全威胁及安全需求。

2.1 CCN 工作原理

CCN 的体系结构与 TCP/IP 的体系结构类似, 均为沙漏型, 如图 1 所示。二者最大区别在于 CCN 中“细腰”部分的内容块取代了 IP, 采用内容名字作为路由标识。CCN 中没有传输层的概念, 但是增加了策略层和安全层。策略层作为网络层的下一层, 为路由提供决策; 安全层作为网络层的上一层, 为网络提供安全性。

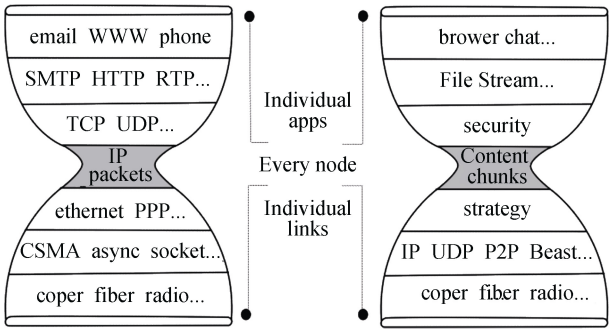

图 1 CCN 体系结构
Figure 1 CCN Architecture

CCN 中有两种数据类型: 兴趣包(Interest Packet)和数据包(Data Packet), 如图 2 所示。

兴趣包(下文根据场景不同也将兴趣包称为兴趣分组)的格式如图 2(a)所示, 包括内容名字、用户选项和随机数。其中, 内容名字表明请求内容的名称, 用户选项表示内容请求者(用户)的特殊需求, 随机数确定接收到的兴趣包是否为之前已经收到的重复兴趣包。数据包(下文根据场景不同也将数据包称为数据分组、数据块)的格式如图 2(b)所示, 包括内容名字、数据载荷、内容发布者的数字签名和相应的认证信息(内容发布者 ID、公钥等)。其中, 数字签名和认证信息用来向内容请求者提供接收内容的完整性保护、准确性认证以及对内容发布者的身份认证。

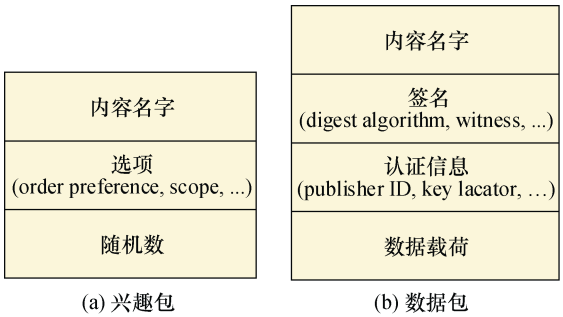

图 2 CCN 包格式
Figure 2 CCN Packets Format

CCN 中的内容获取由内容请求者驱动, 内容请求者通过发送兴趣包来请求相应的内容, 数据按照分块进行传输。在 CCN 中, 用户通过广播方式向周围邻居节点发送包含请求内容名称的兴趣包, 该兴趣包在网内逐步扩散, 当具有该内容的节点收到兴趣包后, 按照兴趣包来时的路径反向回传给用户。在此过程中, 中间路由器节点不仅负责内容传送和转发, 还具有缓存功能。

每个 CCN 路由器(下文根据场景不同也将 CCN 路由器称为 CCN 节点、中间节点、节点、缓存路由器、路由器)维护三个主要数据结构: 内容存储器(Content Store, CS)、待定兴趣表(Pending Interest Table, PIT)和转发信息库(Forwarding Information Base, FIB)。内容请求者向网络中广播兴趣包, 兴趣包中包含所需内容的名称, 路由器记录收到兴趣包的接口, 并通过查找 FIB 的方式转发兴趣包。当兴趣包到达拥有请求数据的节点后, 这个节点会返回数据包, 同时, 发送者的签名也包含在数据包中, 兴趣包和数据包都不会携带主机信息, 如 IP 地址等。兴趣包依据所需内容的名称直接路由到可以提供内容的节点, 而数据包依据兴趣包在转发过程经过的路由器, 原路反向返回给请求者。由于路由器中维护着待定兴趣表, 当多个兴趣包请求同一个内容时, 只有第一个兴趣包被转发, PIT 聚合了其他兴趣包, 并把其到达端口记录在 PIT 的表项中。当数据包到达路由器后, 路由器依据 PIT 表项中保存的端口信息向该端口地址转发数据包, 然后删除这条 PIT 表项, 并把内容分组缓存到路由器的 CS 中, 以便为之后到达的兴趣包提供服务。

通过 CCN 中的数据包转发可以看出, CCN 的设计理念是通信由用户驱动。更具体地说, 每个内容由唯一的分层名称来标识(如“/youtube/videos/ccn.Mpg”), 用户按内容名称通过发送兴趣包请求内容。每个数据包都包含一个数字签名或对它的引用, 在与兴趣包请求时相反的路径上传递。内容发布者计算内容名称和内容本身的签名, 从而将它们彼此链接起来, 同时, 数据包中含有可以检索内容发布者公钥的信息。因此, 数据包被检索到的位置对用户是透明的, 同时用户可以验证数据包的完整性和真实性。另外, CCN 的基本设计特性是网内缓存, 缓存的主要目的是存储高度流行的内容或最近请求的内容。这样, 后续用户可以不用每次都从内容发布者处获取内容, 而是从网络中缓存该内容的路由器获取他们所请求的内容, 这样将极大地减少内容检索的时间和成本。

2.2 CCN 安全需求

CCN 路由和转发基于名称的数据包, 可以消除传统 IP 网络中的四大问题(如 2.1 节所述)。由于主机不需要公开其地址来提供内容, 本地网络也不再需要地址分配和管理, 并且内容命名空间是无限的, 因此 CCN 网络不存在地址转换、地址管理地址耗尽等问题。另外, 内容中心网络架构作为未来互联网的候选者, 它本身就带有安全性设计, 可以抵御多种类型的传统 DoS 攻击[11]。特别地, CCN 通过网内缓存、基于 PIT 的转发、基于名称的路由和转发以及基于内容的安全四个设计, 消除或缓解了传统 TCP/IP 网络中的前缀劫持型攻击(prefix hijacking)、带宽耗尽型攻击(bandwidth depletion)、黑洞型攻击(black-holing)和反射型攻击(reflection attacks)等安全问题。但是, 由于 CCN 独有的 CS 和 PIT 两个特性, CCN 中产生了专门针对 CCN 的新型攻击。

接下来, 将通过分析 CCN 与 TCP/IP 之间的区别, 进一步分析 CCN 中的安全威胁及安全需求。

2.2.1 CCN 与 TCP/IP 的区别

CCN 作为一种新型的网络架构, 与传统的 TCP/IP 网络相比具有以下新特点:

(1) 采用接收端驱动的“拉”模式。接收端通过发送兴趣包来请求内容, 然后, 满足要求的数据源节点返回请求的数据。

(2) 提高了内容分发效率。CCN 中通过中间路由器缓存经过的内容来提高网络中的内容分发效率, 中间路由器中的缓存与 IP 路由器中的缓冲区类似, 都是用来缓存数据包的。但是 IP 路由器将数据包转发之后不能再利用该数据包, 而 CCN 中路由器的数据缓存可以重复使用。

(3) 一个兴趣包对应一个数据包的传输模式。一个兴趣包最多检索一个数据包, CCN 中的路由器通过 PIT 聚合相同的兴趣包, 使得重复的兴趣包只有一个被转发, 这种方式能够实现网络中的流量均衡。

(4) 支持多径路由。传统的 IP 路由通常采用单条最佳路径来防止转发路径产生环路, 而在 CCN 中, 兴趣包中的随机数能够有效地标识重复的兴趣包, 一旦发现收到重复的兴趣包, 便会将其直接丢弃。这种内置的多路径传输机制很好地支持了负载均衡及服务选择功能。

(5) 多源传输。由于 CCN 的内容可以存储在网络中, 因此接收端可以获得由多个内容源响应的内容, 包括来自原始内容发布者和中间节点缓存的内容。

(6) 增强了网络的路由安全。与传统 IP 网络相比, CCN 网络的路由安全性得到大大提高。如网络数据都使用签名机制、有效防范前缀劫持和不能针对特定目标主机或服务器攻击等等。

CCN 的一个关键目标是“设计安全性”[12], 与 TCP/IP 中基于主机的方法不同, CCN 在通信过程中能够保证数据的安全性和完整性[13]。但是, 攻击者可以利用 CCN 独有的两个特性 CS 和 PIT 来进行特定于 CCN 的攻击。

2.2.2 CCN 中的安全威胁及安全需求

CCN 中面临的安全威胁主要分为三类, 分别如下。

1) 用户隐私泄露

CCN 中的隐私泄露问题主要分为两类: 内容隐私泄露和缓存隐私泄露。

• 内容隐私泄露

由于 CCN 中使用内容名称来请求内容, 这些内容名称在语义上与用户偏好相关, 并在网络内传播。因此, 恶意用户基于用户兴趣包可以容易地分析出用户兴趣并获取内容及敏感信息, 这种由于内容本身语义导致隐私泄露的问题称为内容隐私泄露。

• 缓存隐私泄露

CCN 网络中每个节点都可以缓存内容, 即使对内容名字进行保护, 恶意用户仍然可以很容易地获取内容, 并且通过对比缓存和未缓存内容的响应时间差来推断用户请求隐私信息, 这种由于网内缓存机制引起的隐私泄露称为缓存隐私泄露。攻击者通过探测缓存来推测用户行为隐私的攻击称为定时攻击(Timing Attack)。

因此, 要实现 CCN 中的隐私保护, 不仅要保

护网络中的内容隐私, 保证内容的匿名性, 还要保护用户行为隐私, 使得攻击者不能判断用户请求的内容。

2) DoS 攻击

拒绝服务攻击(Denial of Service, DoS)或分布式拒绝服务(Distributed Denial of Service, DDoS)攻击(下文为了方便统一, 统称为DoS攻击)是当今互联网中一个持续存在的问题, 攻击者泛洪大量的数据包使受害机器过载, 从而阻碍网络中的正常数据传输。尽管 CCN 能够抵御多数形式的传统 DoS 攻击(如 2.1 节所述), 但是在CCN中, 攻击者可以利用CCN特有的 CS 和 PIT 两个特性来进行新型 DoS 攻击, 从而耗尽 CCN 路由器或内容发布者中的资源。李杨等[14]分析得出, 在所有针对 CCN 的 DoS 攻击中有两种方式风险最高、对网络影响最大, 一种是兴趣包泛洪攻击(Interest Flooding Attack, IFA), 另一种是缓存污染攻击(Cache Pollution Attack, CPA)。

• 兴趣包泛洪攻击

兴趣包泛洪攻击是指恶意用户通过发送大量虚假名称的兴趣包或流行度非常低的兴趣包来攻击网络, 从而消耗网络的带宽并耗尽路由器的内存。对于攻击者而言, 通过发送虚假名称的数据包进行攻击可以使攻击效果最大化, 而且更易实现[15], 因此几乎所有 IFA 都是通过这种方式进行攻击的, 所以本文中以此为例来讨论兴趣包泛洪攻击。

兴趣包泛洪的目标是使兴趣包传入速率高于从 PIT 中删除条目的速率, 从而使 PIT 饱和。攻击者通过短时间内频繁请求大量不流行的或者不存在的内容, 使得: (1)路由器中的 PIT 饱和, 不能处理合法兴趣包; (2)目标内容发布者瘫痪。一旦 PIT 满了, 因为没有可用的内存为新的兴趣包创建 PIT 条目, 因此所有后续传入兴趣包都将被丢弃。由于内容不流行或不存在, 所以用户的后续请求包不能被满足, 这些兴趣包将保留在 PIT 中尽可能多的时间, 这肯定会耗尽路由器上的内存和计算资源。

• 缓存污染攻击

缓存污染攻击是指恶意攻击者可以通过非常频繁地请求不太流行的内容来伪造内容流行度, 从而破坏这种基于流行度的缓存[16]。

缓存污染攻击旨在降低网内缓存的有效性, 从而降低其实用性。缓存污染攻击特别针对存储在缓存中的流行内容, 并试图用不受欢迎的数据填充缓存, 这迫使用户必须从内容发布者处获取所请求的内容。缓存污染攻击主要分为两种类型[17]: (1)局部中断攻击: 在这种类型中, 攻击者发送大量新的流行度低的内容兴趣包, 从而破坏内容缓存的局部性。由于常用的流行度高的内容会经常被替换, 因此, 网内缓存的实用性会降低。(2)虚假局部攻击: 在这种类型的攻击中, 攻击者重复请求一小组流行度低的内容, 由于攻击者通常会以比合法用户更高的速率请求内容, 因此这一组低流行度的内容很有可能会取代高流行度的内容缓存在网络中。虚假局部攻击可以由恶意内容请求者或内容发布者实施, 恶意内容请求者的目标是改变本地缓存中的内容流行度, 而恶意内容发布者的意图是将其生产的内容存储在路由器的缓存中。需要注意的是, 局部中断攻击和虚假局部攻击不是相互排斥的。也就是说, 攻击者可以进行一种以某种方式结合两种攻击类型的攻击来降低缓存效率并增加内容检索延迟。

由于 DoS 攻击通常易于实例化, 并且攻击通常难以解除[18]。因此, 有效地抵御 DoS 攻击首先需要根据恶意行为检测出攻击者, 然后针对该攻击者的恶意流量进行抑制, 使得网络中的正常流量得到最大程度的保护。

3) 网络拥塞

网络拥塞是指网络中传送的兴趣/数据包太多时, 由于存储转发节点的资源有限而造成网络传输性能下降的情况。虽然 CCN 中的网内缓存和兴趣聚合可以使大量的冗余流量从网络中滤除, 从而显著提高网络性能, 但是拥塞仍然可能发生在这样的网络中, 研究人员需要根据 CCN 的独特性设计新的缓解网络拥塞的机制。

在 CCN 中, 每个兴趣包具有特定的生命周期, 当生命周期到期但没有获得所请求的数据对象时, PIT 将兴趣从表项中移除, 同时内容请求者需要重新发送兴趣包[19]。兴趣包的生命周期可能会由于网络拥塞而到期, 这将导致兴趣包的丢失和重传, 降低网络吞吐量并增加内容传输时延。为了让网络具有更好的服务质量(Quality of Service, QoS), 更好地保证网络可用性, 不仅要进行早期的网络拥塞的预防, 还要在发生拥塞之后控制数据在网络中的传输, 缓解网络拥塞。

3 CCN 中的隐私保护技术研究

目前 CCN 中的隐私保护技术研究主要包括内容隐私保护和缓存隐私保护两类, 其中内容隐私保护又可以细分为内容名称隐私保护和内容数据隐私保护。由于内容隐私保护和访问控制的目的都是防止内容被非法用户获取, 同时两者的核心思想均为给内容加密[20], 因此本文不单独对访问控制进行讨

论, 只以内容隐私保护为代表讨论 CCN 中的内容加密技术。

3.1 内容隐私保护研究现状

文献[21]从三个方面简要讨论了内容隐私的概念。(1)缓存隐私: CCN 中的路由器具有缓存功能, 攻击者可以通过探测内容响应时间来窥探相邻用户的行为隐私, 这种与缓存相关的隐私称为缓存隐私; (2)内容隐私: 由于用户通常使用与内容本身语义相关的内容名称请求内容, 因此攻击者可以通过监视用户请求的内容来获取用户的敏感信息, 这种与内容本身相关的隐私称为内容隐私; (3)签名隐私: 恶意用户可以通过查看签名很容易地推断出内容发布者的身份, 这种与签名有关的隐私称为签名隐私。广义上来讲, 由于内容发布者在数据包中用添加签名的方式来保证内容的完整性和真实性, 如果我们保护网络中传输的内容, 也就保护了签名, 因此, 签名隐私也属于内容隐私的一部分。该文献提出了这三种隐私概念, 但是并没有针对任何攻击情景提出具体的解决方案。

内容隐私保护的方案主要方法是加密, 加密内容在整个网络中传输, 只有授权用户才能解密内容, 非授权用户没有解密密钥就无法解密内容。现存的保护内容隐私的主要方案主要分为三类: 对称加密[22]、广播加密[23]和代理重新加密[24]。

在对称加密[22]中, 用户生成会话密钥并使用内容发布者的公钥对生成的会话密钥进行加密, 内容发布者接收此密钥后, 使用它来加密内容并将内容发回给用户。这种方法使得只有发出请求的用户本身能够解密内容, 虽然能够保护用户隐私, 但却完全禁用了缓存机制, 不能充分发挥 CCN 中沿途缓存的优势。为了解决这个问题, 文献[23]提出一种广播加密方法, 内容发布者使用公钥对内容加密后采用广播形式向用户发送内容, 内容可以缓存在沿路任意节点上, 以实现数据重用, 但是只有私钥拥有者才可以解密内容。该方案的最大缺点就是内容发布者需要维护大量密钥, 影响通信效率。

为了减少要维护的密钥数量, 提高通信效率, 文献[24]提出了一种代理重新加密(Proxy Re-Encryption)的方案。首先对用户身份进行加密, 然后通过代理者(proxy)对密文进行重新加密后在网络中传输。使用代理者重新加密, 用户只需存储与其身份相关联的两个私钥: 一个用于身份加密, 另一个用于代理重新加密。但是缺点是此方案需要进行两次加密, 计算量较大。

为了解决上述三个方案存在的问题, 平衡缓存性能和隐私保护之间的矛盾, 优化缓存性能的同时保护用户隐私, 文献[25]提出了一个名为 PROTECTOR 的方法来保护内容名字和内容, 该方案采用基于代理的加密思想, 用户或节点不共享任何密钥。当用户发送兴趣包请求内容时, 用户会将内容名字中的每个组件转换成相应的陷门(trapdoor), CCN 节点首先重新加密用户生成的陷门, 然后将重新加密的用户请求与节点上存储的加密表格进行匹配。同理, 当内容发布者发送响应数据包时, 将数据包中的内容名字和内容数据转换成陷门, CCN 节点首先重新加密内容发布者生成的陷门, 然后将重新加密后的内容进行存储。该方法使得 CCN 节点可以转发却无法访问内容, 其中用户或节点不共享任何密钥, 同时提供了可扩展的用户密钥管理, 在添加或删除用户时无需重新加密存储在节点上的名字或内容, 因此该方法是可扩展的。但是该方法需要进行两次加密, 在节点执行兴趣匹配和数据存储之前均需要执行加密算法, 计算量仍然较大, 还是会在一定程度上增大网络开销和内容获取时延。

由上述分析可以看出, 实现内容隐私保护技术的难点在于: (1)加密内容后牺牲了 CCN 的缓存能力, CCN 中缓存性能和内容隐私保护之间的平衡问题是 CCN 内容隐私保护方案中有待解决的主要问题; (2)加密过程中需要大量密钥进行多次加密, 计算量较大。未来的工作可以在实现隐私保护的同时, 致力于优化加密算法, 使得耗费的网络开销更小。另外, 区块链作为一种新兴的加密技术, 以分布式及安全性强而闻名, 未来可以用来作为一种新的内容加密方法提高内容安全性。

3.2 缓存隐私保护研究现状

首先结合图 3 更直观地介绍定时攻击。

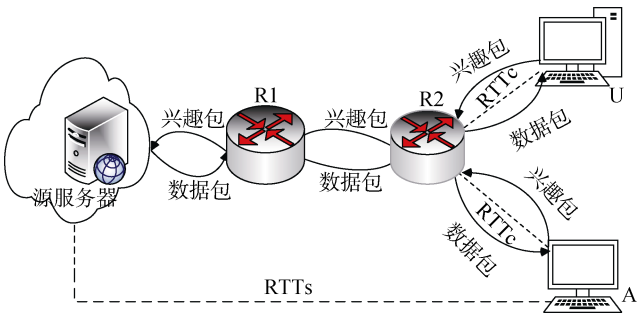

图 3 定时攻击

Figure 3 Timing Attack

假设正常用户 U 是攻击者 A 的邻居用户, 二者共享第一跳路由且服务于同一源服务器。攻击者 A 通过比较不同往返时延(Round Trip Time, RTT)来推

测用户 U 最近是否请求过该内容, 从而探测出用户的行为隐私。攻击者 A 首先测量两个 RTT: (1)RTTs: 攻击者从源服务器处获取未在网络中缓存的内容所需要的往返时延; (2)RTTc: 攻击者从最近的第一跳路由上获取内容所需要的往返时延。当 A 推测目标内容是否已被邻居节点请求过时, 发送对目标内容的请求, 记此往返时延为 RTT, 比较这三个往返时延如下:

• 如果|RTT-RTTc| < ε(ε → 0): A 可以断定目标内容已缓存在最近的路由器 R1 上, 即其邻居用户 U 最近请求过该内容。

• 如果 RTTc < RTT < RTTs: A 推测目标内容最近已被网络中非直接邻居的其他用户请求过并缓存在网络中, 但是, 通过 RTT 和 RTTc 之间的差值大小, A 仍然可以推测出目标内容请求者在网络中的大概位置。

• 如果|RTT–RTTs| < ε(ε → 0): A 可以推测出该目标内容最近未被任何节点请求过。

针对缓存隐私保护中的定时攻击问题, Acs 等[26]提出了一种随机延迟策略来抵御定时攻击, 该方案是为请求的内容增加一个随机的响应时延, 使攻击者将无法推断该内容历史请求者的身份。此方案虽然具有理想的隐私保护能力, 但是它是以完全牺牲 CCN 网络的内容分发能力为代价的。Chaabane 等[27]采用概率缓存的方法来破坏恶意用户定时攻击探测的准确性, 该方案中, 路由器根据自身在内容转发路径上的位置以及缓存中的可用空间来决定是否缓存内容, 此缓存方法基于路由器的内部状态, 因此对手无法知道。但是, 按照概率缓存在路由器上的内容仍然可以泄露用户隐私, 因此该方案的隐私保护能力是非常有限的。以上方法都是以牺牲网络性能为代价来保护缓存隐私, 但是近几年的一些工作旨在解决缓存隐私保护和缓存性能之间的矛盾, 使得设计的隐私保护方案可以在保护隐私的同时提高缓存性能。

文献[28]提出了三种应对定时攻击的解决方案, 每种方案都具有不同级别的复杂性和隐私保护粒度, 这三种方案主要通过添加随机时延来掩饰用户请求。第一种方案让边缘路由器维护所有用户的状态、请求内容的名字以及用户请求次数。当其他用户第一次请求路由器中的缓存内容时, 路由器在将内容发送给请求者之前, 产生随机延迟(根据具有主动学习参数的正态分布)来模拟网络延迟, 从而使恶意用户无法判断所请求的内容是否已在缓存中。此方案实现了细粒度的隐私保护, 但是该方案的一个明显问题是边缘路由器维护的信息量巨大, 造成了非常大的开销。为了减少路由器开销, 在第二种方案中, 路由器维护每个接口的状态而不是每个用户的状态。当某个接口第一次接收到内容请求时, 路由器添加随机时延后发送给用户, 当该接口接收到相同内容的请求时, 则立即发送该内容给用户。此方案以接口为单位保护用户隐私, 与第一种方案相比保护粒变大, 但是明显的减少了路由器开销。为了实现细粒度的隐私保护, 同时减少边缘路由器的开销, 第三种方案维护用户在第一种方案中的相同状态, 但是不是在边缘路由器而是在接入点(Access Point, AP)中维护用户状态。此方案中的接入点是连接用户与边缘路由器之间的一个节点, 专门用作维护用户状态, 标记用户是否是第一次请求内容, 从而根据与第一种方案相同的方法响应用户请求。

上述三种方案中, 无论是路由器还是接入点维护用户或接口状态, 都会产生一定的开销, 一定程度上影响通信效率。为了减少更多的网络开销, 降低路由器维护用户状态的压力, 文献[29]提出了一种基于最近访问信息与回退机制的缓存隐私保护策略, 该策略中定义了一种新的判断用户请求次数的方法, 具体如下: 路由器针对隐私内容设置隐私标识, 并在隐私标识中存储该隐私内容的最近访问时间。用户在发送兴趣包时, 在兴趣包的 nonce 字段内置入上次访问时间, 当兴趣包到达路由器时, 路由器提取其中的 nonce 字段, 将 nonce 中的时间与该内容隐私标识内的最近访问时间对比。如果基本接近, 则判断为兴趣包发送者是该内容上一次的请求者, 直接返回数据包且将隐私标识更新为当前访问时间。如果时间相差较大, 则判断为兴趣包发送者是新的请求者, 路由器将内容隐私标识中的最近访问时间更新为当前访问时间, 同时延迟随机时间再发送数据分组给请求者。另外, 当请求未被命中且请求对象为隐私内容时, 路由器在获取该隐私内容后, 不采用常规的 LRU(Least Recently Used)策略将该内容置换到缓存队列首部, 而是随机将该内容存入缓存中的任意位置, 同时从存入位置开始至缓存队列尾部为止的所有内容按顺序向后移动一位。当内容(包括隐私内容与非隐私内容)被移出当前路由器缓存队列时, 以概率 p 回退上一层节点存储(同时以概率 1-p 直接丢弃), 存入上一层节点缓存的队列首部。这一随机存入操作, 可以使得攻击者无法估计所请求内容在缓存中的停留时间。此方案为判断用户是否是第一次请求某内容提供了一个新思路, 可以在降低隐私泄露概率的同时, 一定程度上提高网络性能。

以上方案均使用用户第一次请求时添加时延的方式混淆攻击者的判断, 但是这些方案有一个共同的缺点, 即对正常用户的内容获取造成了一定的影响。因为凡是第一次请求的内容, 无论是正常用户还是恶意用户, 均被添加了随机响应时延, 这固然保护了用户隐私, 但是对正常用户的内容获取也增加了时延。为了减少对正常用户的影响, 文献[30]提出匿名区域的概念, 通过网络内节点协同缓存机制来增加攻击者探测的不确定性。该机制的主要思想是扩大匿名区域从而增大攻击者推测的不确定性, 将内容缓存在沿途最大的热点缓存区域, 避免冷门资源的缓存, 并在匿名区域所属节点基于一致性哈希实现内容的协同混淆存储, 增大攻击者推测的难度和不确定性, 从而实现缓存内容的隐私保护。

以上研究主要针对一般文件或内容进行保护, 还有一些研究者针对特定业务或应用场景进行研究。例如, 文献[31]提出一个针对视频流量的新颖的混淆攻击者判断的方法—CodingCache 多路径缓存方案。该方案采用网络编码和随机转发的方式, 利用 CCN 中多径路由的特性, 可以改善不同路径缓存内容的多样性和内容请求者的匿名性。为了实现高性能的多径路由, 此方案使用随机线性网络编码(Random Linear Network Coding, RLNC)将多个视频内容块编码成一个块, 编码块可以服务于由编码块构成的任何原始块的请求。在 CodingCache 中, 视频内容的线性独立编码块被缓存在服务器和内容请求者之间不同路径上的路由器上, 这样可以改善不同路径上的缓存内容的多样性, 还可以优化缓存性能以及保护原始请求者的隐私。

当 CCN 用于电子商务或银行业时, 安全比缓存更重要, 因此可以以牺牲缓存为代价来换取安全。文献[32]提出一种针对这种情况的新方法, 请求和响应都需要语义或选择密文安全(Chosen Ciphertext Security, CCA-security) 加密, 受传输层安全协议 TLS1.3[33] 的启发, 该文献提出了名为 CCNxKE (ICNs–CCNx Key Exchange)的方案。CCNxKE 使内容请求者和内容发布者使用前向安全密钥创建安全会话, 以使用 CCA-security 加密方案对请求和响应进行加密。CCNxKE 协议允许两个对等体建立共享的前向安全密钥, 以进行安全和保密的通信, 它旨在防止两个对等体之间的窃听, 篡改和消息伪造, 同时最小化建立共享密钥所需的轮次数。此协议在最大程度上保证了通信的安全性, 不过此过程中的会话加密和消息封装交换会话信息等操作, 不仅破坏了 CCN 中的缓存优点, 而且带来了很大的网络开销和计算复杂度, 一般只在对安全有非常严格要求的场景下应用。

由以上总结可以看出, 缓存隐私保护技术的难点在于: (1)路由器维护的信息量巨大将会导致网络开销过大; (2)添加内容响应时延会影响正常用户的用户体验。未来的工作可以集中在使用更加有效的方式混淆攻击者使其无法识别正常用户请求, 如利用移动目标防御技术(Moving Target Defense, MTD)。另外随着机器学习和深度学习技术的不断发展, 未来可以用机器学习的方法通过分析用户行为来识别恶意用户, 从而只针对恶意攻击者采取防御策略, 更大程度上减少对正常用户的影响, 在保护正常用户隐私的同时优化网络性能。

3.3 二者兼顾的隐私保护方案

柳毅等[34]提出一种基于多层加密机制的内容中心网络隐私保护策略, 该机制不仅实现了内容的加密传输来保证内容隐私的安全, 还通过在兴趣包中添加 LastTime 字段来防止邻居用户恶意窥探用户请求。为了抵御定时攻击, 当兴趣包到达 CCN 节点时, 兴趣包中的 LastTime 字段与缓存内容的最近访问时间字段做比较, 若两字段基本接近, 则说明该用户不是第一次访问该内容, 直接返回内容给用户, 并修改该内容的最近访问时间为当前访问时间。若两字段相差较大, 则说明此用户为第一次请求该内容, 添加随机时延再发送给用户, 并更新内容最近访问时间字段。同时, 该方案通过对内容进行多层加密来保护内容安全。该方案采用洋葱路由的思想和非对称加密的方法, 使用发布者公钥、下一层路由器公钥加密内容, 每一层路由器都可以使用自己的私钥解密内容。为了避免攻击者窥测到用户的请求, 兴趣包用哈希值来代替。另外, 此方案使用数据填充来保持内容的长度不变, 防止攻击者根据内容的长度变化来判断内容所在位置。该方案在实现隐私保护的同时保持了路由器的缓存优势, 同时减轻了路由器维护大量密钥的负担并提升了请求者的可信度。但是很明显, 该方案中每个节点存储和转发内容时均需要一次加解密操作, 这虽然很好的保护了缓存隐私, 但也带来了一定程度的计算开销并增加了用户内容获取时延。

表 1 给出了几种典型隐私保护方案的对比。

4 CCN 中的 DoS 攻击技术研究

4.1 CCN 中的兴趣包泛洪攻击技术研究

结合图 4 介绍兴趣包泛洪攻击。

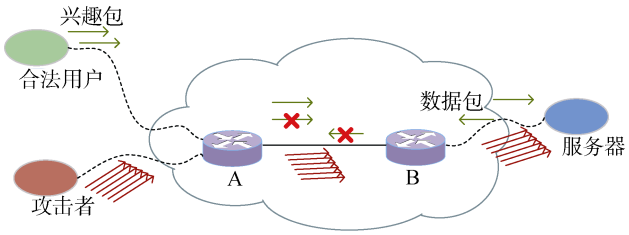

图 4 兴趣包泛洪攻击

Figure 4 Interest Flooding Attack

如图 4 所示, 攻击者通过向网络中注入过多的兴趣包来使网络超载, 从而导致合法用户的服务被中断。由于CCN中是基于名称前缀的路由, 因此DoS攻击者可以泛洪一个特定的名称空间的兴趣包来占用网络资源, 从而使网络瘫痪。如图 4 中, 如果内容发布者是“/ foo / bar”名称空间的独占所有者, 则路由器 B 和内容发布者将收到所有“/ foo / bar / ...”的兴趣包, 并回复响应数据。大量此类恶意兴趣可能会以两种方式破坏 CCN 网络的服务质量: (1)造成网络拥塞。与传统网络类似, CCN 中的兴趣包转发会消耗网络流量, 大量兴趣包可能会导致拥塞并使合法兴趣包在网络中丢失。(2)耗尽路由器资源。由于 CCN 路由器中用 PIT 条目来维护每个转发兴趣包的状态, 因此过量的恶意兴趣包会导致路由器内存耗尽, 使得路由器无法为新传入的合法兴趣包创建新的 PIT 条目, 从而无法为正常用户提供服务。

表 1 隐私保护方案对比

Table 1 Comparison of the Privacy Preserving Schemes

方案	保护对象	保护方法	网络开销	缓存能力
文献[22]	内容	对称加密	加解密开销, 较小	完全丧失
文献[23]	内容	广播加密	内容发布者维护大量密钥, 开销大	较强
文献[24]	内容	代理重新加密	密钥少, 计算量大, 开销较大	弱
文献[25]	内容	代理加密	不共享密钥, 两次加密, 开销较小	强
文献[26]	缓存	添加随机响应时延	较大	强
文献[27]	缓存	概率缓存	小	弱
文献[28]	缓存	(1)路由器维护用户状态信息, 添加随机时延; (2)路由器维护接口状态; (3)接入点维护用户状态	(1)路由器开销大; (2)较大; (3)较小	(1)强; (2)较强; (3)强
文献[29]	缓存	兴趣包记录最近访问时间, 同时使用回退机制	较小	强
文献[30]	缓存	协作缓存, 扩大匿名区域	小	强
文献[31]	缓存和内容	网络编码; 随机转发	小	强
文献[32]	内容	使用前向安全密钥创建安全会话	大	几乎丧失
文献[34]	缓存和内容	最近访问时间和对称加密	较大	较强

针对兴趣包泛洪攻击, 文献[35]指出, 抵御 DoS 攻击不仅要检测攻击者的恶意行为, 还要阻止恶意网络流量。因此, 现有抵御兴趣包泛洪攻击的方案主要专注于检测攻击和对攻击进行防御两个阶段的对策[36]。

Gasti 等[11]提出了抵御兴趣包泛洪攻击的主流思路: 路由器统计策略和回推机制。(1)路由器统计策略: CCN 路由器跟踪过期兴趣, 并使用这些过期信息来限制每个输出接口的未决兴趣数量、每个传入接口的兴趣和每个名字空间的未决兴趣数量, 利用路由器中维护的兴趣包状态来有效缓解 DoS 攻击。(2)回推(push-back)机制: 当路由器怀疑某个特定名称空间正在被攻击时(比如当具有某个名称空间的兴趣包数量在给定接口上达到该名称空间的 PIT 数量极限时), 路由器将限制该命名空间的任何新兴趣的接收和转发, 并将此事件报告给该接口上连接的路由器。这些路由器将攻击信息沿反向路径向下传输到发出攻击的接口处, 限制被攻击的名称空间兴趣转发的速度。回推机制可以将一次攻击推回到其源头, 或者至少推到可检测到的位置, 从而尽可能地从源头限制攻击, 但是本篇文章并没有给出两种方案具体的实现机制。

文献[37]实现了与回推机制类似的兴趣包回溯(Interest trace back)方案, 可以用来识别攻击者, 并抵御兴趣泛洪攻击。路由器伪造数据包以满足攻击者所请求的不存在的内容, 根据 CCN 中数据包传回与兴趣包传输路径对称的原则, 在 PIT 的帮助下, 伪造的数据包最终传回到攻击者节点, 路由器就能定位攻击者节点。识别攻击者之后, 通过限制与此攻击者相连的路由器接口的兴趣包传入速率来减少传入网络的攻击兴趣包, 达到抵御兴趣包泛洪攻击的目的。

检测攻击可以是本地检测或分布式(协作)检测, 在前者中, 路由器仅依靠本地参数指标(例如, PIT 使用率、未被满意的兴趣包率等)来识别攻击; 在后者中, 附近的路由器协作确定攻击是否正在进行以及如何缓解攻击。通过协作检测, 路由器不仅可交换有关攻击存在的信息, 还可交换此类攻击的属性, 从而使得应对攻击的策略可以兼顾来自多个路由器的反馈。

基于回推机制以及分布式检测方法, Compagno 等[38]提出一种名为 Poseidon 的方案, 该方案使用路由器协作检测方式来对抗兴趣泛洪攻击。Poseidon 是一组在路由器上运行的算法, 目标是识别流量异常(特别是兴趣包泛洪)并减轻其影响。Poseidon 持续监控每个接口在整体流量方面的不满意兴趣(unsatisfied interests)所占比率, 如果这些速率在两个连续的时间间隔内差异非常大, 它会在这个异常接口设置一个过滤器来使传入兴趣的数量减少。另外, Poseidon 还利用回推机制向接口发出“警报”消息, 提醒接口正在发生兴趣包泛洪攻击。Poseidon 还保留了一些关于过期兴趣的统计数据, 分别记录名称空间和输入/输出接口信息, 为抵御攻击提供更多信息。

文献[39]从一个全新的角度出发, 指出 CCN 在每个路由器上存储每个数据包状态的固有属性并保持流量均衡(即, 一个兴趣数据包最多检索一个数据数据包)为有效地抑制 DoS 攻击提供了基础。基于流量均衡的原则, 论文提出了三种缓解兴趣包泛洪攻击的算法: 每个接口公平的令牌桶机制、基于满意度的兴趣转发机制和基于满意度的回推机制, 利用路由器状态信息来抵御兴趣包泛洪攻击, 这三种方案的复杂度递增, 抵御泛洪攻击的有效性也递增。

• 每个接口公平的令牌桶机制(token bucket with per interface fairness)

抵御兴趣包泛洪攻击的最直观的解决方案是限制通过网络转发的兴趣数量, 为此, 每个接口公平的令牌桶机制利用兴趣包和数据包之间流量平衡的基本原则, CCN 路由器根据相应接口的物理容量限制每个接口转发的兴趣数量。类似于 IP 中的令牌桶算法(通过以一定速率向令牌桶中增加令牌, 路由器转发数据消耗令牌的方式来控制发送到网络上的数据的数目), CCN 路由器可以根据转发的兴趣包的数量估算出下游链路的数据包数量, 一旦达到链路容量限制, 就不再转发新的传入兴趣。这种算法的最大缺点是 DoS 攻击仍然可能发生, 因为如果路由器利用其所有令牌转发恶意兴趣, 就不能再转发来自合法用户的兴趣。作者解决此问题的方法是强制每个接口的公平性, 以便恶意兴趣不能完全消耗特定接口的资源。

为了确保实现来自所有相邻节点的兴趣包公平转发的目标, 此方案扩展了 PIT 来标记不能立即转发的兴趣包, 并为每个接口实现分层队列。这种机制基本上是一个基于类的排队[40], 每个输出和输入接口都有类, 路由器要保证与输出接口相关联的令牌在每个输入接口之间公平分配。与正常排队不同的是, 这里的兴趣队列并不存储实际的兴趣包, 而仅仅是一个指向现有 PIT 条目的双向指针。因此, 当实际转发兴趣包时, 可以快速更新 PIT 条目, 并且在兴趣包到期时能够容易地将该元素从队列中移除。尽管这种算法对于确保 CCN 网络中有限的公平性是合理的, 但是攻击者仍然可能占据网络中所有流量, 因此该方案在保护合法用户免受恶意攻击方面效果不大。

由以上方案可以看出, 要想抵御兴趣包泛洪攻击, 就必须能够在某种程度上检测并区分来自攻击者的恶意请求。因此, 该文献提出以下两种方案。为了区分合法兴趣和恶意兴趣, 作者利用 CCN 架构的另一个独特功能——兴趣包和数据包的流量是对称的, 由于数据包采用了相应兴趣包的反向路径, 所以路由器可以监测每个兴趣包是否最终获取到响应数据。由于恶意虚假兴趣不可能有对应的数据返回, 因此路由器可以利用此信息区分恶意和合法流量。路由器可以主动维护兴趣满意率(Interest satisfaction ratios)(满意兴趣(satisfied Interests)数量与转发兴趣(forwarded Interests)总量之比)的最新统计数据, 并使用这些统计数据来确定应该转发还是放弃传入的兴趣。

• 基于满意度的兴趣转发(satisfaction-based Interest acceptance)

基于满意度的兴趣转发是指采集兴趣满意度的统计数据, 利用兴趣满意率来惩罚恶意兴趣, 实现惩罚的直接方法是将兴趣满意率直接作为转发或丢弃传入兴趣的概率。该方法的缺点是会产生过度反应, 因为路径上的每个路由器都会独立决定是转发还是丢弃兴趣, 随着跳数的增大, 兴趣包被转发到下一跳的可能性会显著降低。防止这种过度反应和不公平处罚的一种方法是路由器之间交流协作, 诸如相邻 CCN 路由器之间通过 gossip 协议互相交流信息可能会缓解该问题, 但该文章并没有实现解决这个问题的方法。

• 基于满意度的回推机制(satisfaction-based pushback)

基于满意度的回推机制是指采集兴趣满意度的统计数据, 利用满意度比率回溯到攻击源并显式通知周围路由器, 从而达到抑制恶意兴趣的转发的目的, 这种缓解算法能够有效地抑制攻击并确保几乎所有合法兴趣都得到满足。此算法开始时满意率急剧下降, 因为所有路由器都需要几秒钟才能充分意识到攻击。但是, 随着恶意兴趣开始超时并且显式兴趣限制通告开始成功地将恶意兴趣限制在攻击者附近, 因此满意率恢复很快, 一旦恶意兴趣被有效抑制, 合法用户的所有兴趣都将得到满足。基于满意度的回推机制可以有效地抑制攻击, 但是此方案只是在一个简单和静态的攻击者模型情境下实施的, 它不考虑中间路由器的缓存, 而是一直将用户兴趣转发给内容发布者。

为了应对新型的 DoS 攻击和未知的攻击以及异常威胁, 许多研究人员指出, 智能学习技术可以作为当前 DoS 攻击检测研究的重要组成部分[41]。预测 DoS 攻击的一种流行方法是使用人工神经网络(Artificial Neural Networks, ANNs)分类[42], 人工神经网络已成为解决许多复杂实际问题中最重要、最有价值的工具之一[43]。其中, 径向基函数(radial basis function, RBF)神经网络可以直接通过输入和输出数据来预测用户行为[44], 而且目前已成功地用于解决动态系统问题。基于此, Karami 等[45]提出了一种智能混合算法, 用于主动检测 DoS 攻击和自适应反应(防御)。在检测阶段, 文中应用了多目标优化和粒子群优化(Particle Swarm Optimization, PSO)的 RBF 神经网络的组合来获取更准确的基于 RBF 网络的分类器(预测器), 并利用这个优化的预测器来主动检测 CCN 中的 DoS 攻击, 这种方法包括两个阶段: 训练阶段和预测阶段。在训练阶段, 利用多目标方法和 PSO 在 RBF 神经网络设计中的实现来提高分类问题的准确性。同时, 应用 Deb 等[46]提出的非支配排序遗传算法(Non-dominated Sorting Genetic Algorithm, NSGA II)通过 DBI(Davies–Boulding Index)[47]确定 RBF 单元中心的分离中心的 Pareto 解, 并基于均方误差(Mean-Square Error, MSE)[48]对其进行局部优化。然后, 通过使用 PSO 完成单位宽度和输出权重的优化和调整, 其中每个粒子编码一组宽度和权重。而且, 这个步骤很简单, 易于实施, 但是在指示多个性能指标方面非常有效。在预测阶段, 采用一种简单的算法, 以最小的错误分类概率对新输入模式的有效性进行分类。在防御阶段, 通过对攻击者实施明确的限制来执行简单的自适应反应算法, 使 CCN 路由器能够快速有效地对网络问题进行自适应反应, 以保证合法的数据传输性能并有效地抑制恶意用户的流量。基于神经网络的智能算法是比较灵活且抵御攻击效果比较好的一种方法, 运行智能算法的前提是训练出正常网络状态下的流量传输模式。但是由于现实网络运行过程中用户流量可能是动态变化的, 所以难免会有结果不准确的情况出现。解决此问题的一个思路是周期性地训练, 但是这又会引起网络中的巨大的计算开销和网络延迟。

近几年, 许多研究人员针对 CCN 中的一些特定应用场景提出了兴趣包泛洪攻击的防御策略, 本文主要介绍两个应用场景下的防御策略: 基于 CCN 的无线多媒体传感器网络(Wireless Multimedia Sensor Networks, WMSN)和基于 CCN 的车载网络。

由于 WMSN 的广播性质, 数据包泛洪是一个热门的研究问题, 因为在基于 CCN 的 WMSN 中, 采用无线广播方式进行数据传输, 数据包流的方向不能被控制, 以致过多的兴趣包泛洪从而导致下载内容的延迟。为了缓解这个问题, Chan 等[49]利用传统 CCN 的优点, 针对智能城市的基于 CCN 的 WMSNs 提出了一种新的协议, 称为分组有限扩散协议(packet diffusion-limited protocol, PDLP)。在 PDLP 中, 转发兴趣包的方式与以内容为中心的多跳无线增强网络(Enhance Content-Centric Multihop Wireless Networks, E-CHANET)[50]相同。不同点在于, 无论节点何时转发兴趣包, 它们都将其 MAC 地址添加到兴趣包中。PDLP 的兴趣包末尾添加一个 MACAddrList 字段, 该字段包括内容请求者转发至内容发布者过程中所有中间传感器节点的 MAC 地址。当一个中间传感器节点收到一个兴趣包并决定进行转发时, 它会在该字段中添加其 MAC 地址。因此, 当兴趣包被转发到内容发布者时, MAC 地址在该字段中被累积, 字段的大小根据在兴趣包到达提供者之前经过的节点数量而变化。同时, 该字段也被添加到数据包中, 内容发布者在发送数据包之前, 将兴趣包字段中的 MAC 地址列表复制到数据包字段。当一个节点接收到数据包并且其地址在该字段中时, 它从数据包的地址字段中删除其 MAC 地址。同时, 数据包中还添加了 MaxHopCnt 和 HopCnt 字段, MaxHopCnt 字段记录了 MAC 地址的数量, 表示从内容请求这到内容发布者之间的节点数量, HopCnt 字段表示当前数据包还可以被转发多少跳。与在无线自组织网络中使用的常见单播路由协议不同, 该方案中的数据包是在最短路径周围的一个限制区域内传输。因此, 该方案不仅限制了一定程度的数据包泛洪, 而且可以缩短在内容发布者到内容请求者的最短路径范围内的内

容下载时间。因此, 当 CCN 应用在有线网络中时, 可以利用路由器接口等网络信息控制兴趣包泛洪攻击; 当 CCN 应用在无线网络中时, 可以利用网络中节点的 MAC 地址来将兴趣包泛洪控制在一定范围内。

文献[51]提出一种基于 CCN 的车载网络中的 Dos 攻击片段认证方法。通常情况下, CCN 数据包根据内容传送路径的最大传输单位(Maximum Transmission Unit, MTU)大小进行分段和重新组合, 但是, 该文章提出了一种新的安全内容分片方法, 通过在路由路径上的临时节点处进行即时片段验证来保证每个片段的真实性。该方法的主要创新点在于提出一种新的哈希树结构, 它将纠删码(用于前向纠错)无缝集成到哈希树中。该方案提出的哈希树在接收时使每个片段具有很高的即时可用概率, 同时, 为内容片段设计了一种自适应转发策略, 使得节点在收到片段后无法立即确认其真实性。路由器通过根据最近观察到的真实与不真实片段的比例自适应调整这些片段的转发概率, 这样可以在良性环境中快速传播合法片段, 同时有效地消除恶意环境中的非法片段。

由以上分析可以看出, CCN 中的兴趣泛洪攻击检测与防御策略的难点在于限制异常接口的转发能力时会误伤正常用户, 因此正逐渐向智能化方法发展, 以期更好的识别恶意流量, 从而减少对正常用户或流量的误伤。未来工作中可以更好地利用神经网络中的一些与时俱进的新算法, 如基于深度学习的用户画像算法、基于 BP(Back Propagation)神经网络的用户行为分析算法等等, 从而达到更好的恶意流量识别效果, 在根源上抑制洪泛攻击。

表 2 给出了几种典型兴趣包泛洪攻击检测和防御策略的对比。

表 2 兴趣包泛洪攻击检测与防御策略对比

Table 2 Comparison of Interest Flood Attack Detection and Defense Strategies

方案	攻击检测方法	检测粒度	对抗方法	对抗粒度	开销	部署位置	对正常用户影响
文献[11]	路由器统计兴趣包过期率	异常接口	限制输出接口的兴趣并回推	按接口限制特定命名空间	中	全网路由器	大
文献[37]	PIT 使用率	异常名称	回推并限制兴趣包传入速率	按攻击者限制接口处的传入速率	小	特定位置	中
文献[38]	PIT 过期兴趣率	异常接口	接口设置过滤器并回推	按接口限制	大	全网路由器	小
文献[39]	(1)路由器兴趣转发率 (2)PIT 满意率 (3)PIT 过期率	异常接口	(1)限制异常接口兴趣转发速率 (2)基于兴趣满意率限制兴趣速率 (3)回推并限制源处兴趣速率	按接口限制	(1)大 (2)中 (3)小	全网路由器	(1)大 (2)中 (3)小
文献[45]	RBF 神经网络智能算法	异常用户	限制恶意用户的传入流量	按用户限制	大	全网路由器	小
文献[49]	节点添加 MAC 地址到兴趣包	-	-	-	小	无线网络	小
文献[51]	临时节点验证内容片段	内容名称	调整内容片段转发速率	按内容名称限制	中	全网路由器	小

4.2 CCN 中的缓存污染技术研究

为了有效且高效地抵御缓存污染攻击, 一方面, 如果攻击早期(造成高度破坏之前)可以抑制攻击, 则可以认为防御机制是有效的(effectively)[52], 另一方面, 如果防御机制以最小的花费实现安全保护, 则可称为是高效的(efficiently)[53]。但是, 防御机制的有效性和高效性是相互矛盾的, 要实现防御机制的有效性意味着每个节点都应该具有最新的全网信息视图, 这需要非常频繁地协调网络中的节点间通信。但是, 网络层面的协调会耗费大量的网络流量, 而且需要耗费巨大的存储空间和处理能力[54], 因此抵御缓存污染攻击的关键是要协调算法的有效性和高效性。如 2.3 节所述, 缓存污染攻击分为局部中断攻击和虚假局部攻击, 以下详细介绍针对这两种类型攻击的防御策略。

4.2.1 局部中断攻击对策

Park 等[55]提出了基于随机性检查的缓存污染检测方案, 此方案利用矩阵排序和序列分析来检测低速率缓存污染攻击。假设攻击者以低速率请求数据块来绕过所有速率过滤器(过滤掉以高速率请求的攻击者流量), 在该检测方案中, 首先路由器将其 CS 中的内容映射到 $n\times n$ 二进制矩阵中, 然后使用两个密码散列函数将内容名称映射到矩阵中的位置并评估其排名 M, 排名过程重复 k 次, 如果矩阵排名达到预

定义阈值, 则触发攻击警报。此方案专注于低速率攻击, 在检测低速率局部中断攻击方面是有效的, 但是该方案在缓存路由器上的计算量很大, 局部干扰抑制方法需要在中间路由器的每个内容缓存决策中进行复杂计算和迭代, 会导致大量的计算量开销。

文献[56]提出一种 CacheShield 方法, 该方法利用了正常请求和恶意请求之间的特征差别, 由于正常的 Web 请求遵循 Zipf 分布[57], 但恶意请求通常遵循均匀分布, 因此利用二者的区别来进行恶意流量识别。当请求内容未在 CS 命中时, CacheShield 运行一个屏蔽算法, 主要目的是阻止不流行的内容对象在 CS 中被缓存。为了防止攻击者预测到缓存决策, 使用概率函数作为屏蔽函数, 该函数计算每个请求的内容对象的缓存概率, 内容对象被请求的次数越多, 内容被缓存的概率就越高。CacheShield 主要针对难以检测到的局部中断攻击, 可以使用不同的缓存替换策略来实施, 增强了缓存的鲁棒性。另外, CacheShield 很简单, 易于部署, 不需要不同管理域之间的协调, 不需要在同一个域中的不同 CCN 路由器之间进行协调。但是, CacheSheild 的一个缺点是节点需要存储大量统计信息, 占用大量的网络空间。

上述两种方案都会消耗大量的网络资源, 为了解决高开销的问题, 有些方案仅使用路由器中的一部分内容来进行攻击检测。Conti 等[58]提出了一种检测缓存污染攻击的轻量级机制, 该算法由学习步骤和攻击测试步骤组成。该机制首先运行一个学习阶段, 它在攻击发生之前定义内容请求者请求内容的随机样本集, 之后监视这个集合来确定攻击是否正在进行。学习步骤会识别评估内容的攻击阈值(定义为 τ), τ 的值由攻击测试步骤使用。攻击测试步骤计算出的 τ 与另一个值 δ_m 进行比较, δ_m 值是样本集中所有内容的参数(例如内容请求频率和测量间隔的大小)的函数, 如果 δ_m 大于 τ, 则该机制检测到攻击。该机制能够通过各种网络拓扑相对快速地检测高速缓存污染攻击, 但是它只能检测到攻击, 却不能识别出攻击兴趣或内容块, 而且也不具有防御功能。此外, 由于内容流行度的分布在实际网络中可能会不断变化, 因此该机制不能实时地根据实际网络状况进行精确检测。受上述文章的启发, 文献[59]提出了优化方案使其能够识别出攻击者请求的内容前缀。此方法通过仅存储内容的前缀而不是全名来减少存储空间的消耗, 而且该方案还为被识别为攻击的内容前缀设置了一个黑名单用于在防御阶段阻止恶意流量的传输。但是该方案具有很大的局限性, 因为只有当攻击者用正常用户通常不使用的一小部分前缀请求内容时, 这个方法才能正常工作。如果攻击者请求一组用流行内容名称前缀的一部分组成的不流行内容名称前缀的内容, 就可以绕过这个检测方案。而且, 如果该前缀被添加到黑名单中, 甚至就会影响正常用户的内容获取, 缓存的有效性会被降低。

除了上面讨论的限制和问题之外, 上述检测和防御机制仅在节点级别上工作, 每个节点单独检测高速缓存污染攻击, 而不与其他节点协作。因为单独的每个节点只能对可以检测到的攻击特征(例如, 内容请求速率、缓存有用性或内容请求模式)进行严格限制, 因此, 早期的攻击检测和预防可能无法实现, 特别是对于分布式攻击。此外, 在节点之间没有协作的情况下自主防御潜在攻击可能会限制合法流量, 造成过度防御。为了克服这些问题, Salah 等[60]提出一种 CCN 中的轻量级协作框架 CoMon++, 使用节点间协作方式进行攻击预防和检测。CoMon ++不是依赖单个节点上统计的网络信息, 而是攻击相关的全网视图, 该方案通过一小部分网络节点捕获全网视图。CoMon++选择一些相对靠近用户的节点作为监视节点(Monitoring Node, MN), 这些节点协作能够捕获攻击相关信息的全网视图(如内容请求速率和 ISP 内命中率), 利用这些信息的汇总以节点间协作的方式抵御缓存污染攻击。CoMon++在一个 ISP 中工作, 该 ISP 由一组通过边集 E 连接的节点组成, 每个 ISP 具有从 MN 接收统计的集中控制器。ISP 控制器(ISP Controller, IC)汇总这个统计数据, 然后发送 ISP 范围的内容请求信息给 MN 和其他节点。除了常规神经网络的功能之外, MN 持续监测传入数据包及其 CS, 并将其监测信息汇总后发送给 IC。同时, MN 也收到来自 IC 的与 ISP 有关的攻击相关信息, 并随后采取相应的措施。CoMon++使用基于覆盖的路由和靠近源的放置(Placement based on covered Routes and Closeness to Sources, PRCS)的贪婪算法选择 MN, 使得通过 MN 的唯一路由的数量最大化, 并且同时给用户终端附近的节点赋予优先权, 以便 MN 可以在攻击早期阶段抵御攻击。另外, CoMon++中的信令开销非常低, 因此网络开销不是很大, 一定程度上解决了开销问题。

4.2.2 虚假局部攻击对策

文献[61]研究了 ICN 中缓存污染攻击的可扩展性和有效性, 并探讨攻击可能成功的情况。基于此, Karimipoor 等[62]使用 python 实现了 ICN 架构, 并且使用 FIFO 和 LRU 缓存策略模拟缓存污染攻击, 分析了不同规模网络下攻击的有效性, 通过比较正常系统和缓存污染攻击下的系统来研究网络性能。该方

案定义了不同的缓存大小和策略, 以查看攻击对小型网络与大型网络的影响, 还研究了不同的攻击和攻击检测概率对网络的影响。与传统 ICN 网络用 Zipf 分布模拟缓存服务不同, 该方法用 Python 函数创建了具有指数分布的随机请求, 将热门内容放入缓存中。但是, 这项研究工作主要集中在评估缓存污染攻击的有效性以及在发生虚假局部攻击时执行性能分析, 并没有给出任何针对缓存污染攻击的检测和防御机制。

Karami 等[63]提出了一种基于自适应神经模糊推理系统(Adaptive Network-based Fuzzy Inference System, ANFIS)的高速缓存替换策略来缓解高速缓存污染攻击, 该策略分为三个阶段: 输入输出数据模式提取, 构建的 ANFIS 结构的准确性验证, 以及将结构集成为缓存替换策略。此机制可以有效提高网络中的缓存命中率, 但是, 这种机制需要存储每个缓存内容的历史和统计信息, 需要巨大的内存开销, 而且统计的迭代计算会降低可伸缩性。

为了解决高开销问题, Mauri 等[64]讨论了 CCN 中的高速缓存污染情况, 作者假定攻击场景是恶意内容发布者操纵一些终端节点来请求其内容, 目的是破坏路由器的缓存从而优先存储自己的内容来降低内容传输延迟。这种做法会导致攻击者的内容目录中较大部分向下移动到网络边缘, 从而改善了目标内容的传输延迟。作者提出了一种针对此攻击的缓解机制, 该机制使用安装在攻击者附近的蜜罐, 监视用户兴趣包并向上游路由器报告恶意兴趣。路由器将这些兴趣包集中到黑名单中, 这个黑名单中的兴趣包被使用标准的 CCN 路由协议传送给内容发布者, 而不是被传送到距离其最近的路由器。该方案在路由器上引起较低的计算开销, 但是, 它需要额外的基础设施。

由于缓存污染攻击是破坏缓存的攻击, 因此抵御此类攻击的未来研究方向可以从缓存放置策略和缓存替换策略两个缓存机制着手, 设计出更加强大稳定的缓存机制来防止攻击对缓存的破坏, 同时改善网络性能。比如可以在设计缓存机制时将缓存污染攻击的防御考虑进去, 根据网络的动态变化, 当缓存污染攻击发生时能够进行自适应反应来抵御攻击, 而且可以通过高速缓存之间的协作缓存和反馈, 路由器之间可以交换缓存状态和缓存的内容流行度, 以减少不流行内容的缓存[65]。

表 3 缓存污染攻击检测与防御策略对比

Table 3 Comparison of Interest Flood Attack Detection and Defense Strategies

方案	适用攻击类型	检测方法	检测粒度	对抗方法	对抗粒度	开销	部署位置
文献[55]	局部中断攻击	矩阵排序和序列分析	异常接口	限制兴趣包转发速率	按接口限制	大	全网路由器
文献[56]	局部中断攻击	兴趣包请求分布规律的异常	异常内容名称	设置存储阈值, 限制不流行内容的缓存	按节点限制	中	边缘和核心路由器
文献[58]	局部中断攻击	机器学习方法计算攻击阈值	异常接口	-	-	大	全网路由器
文献[59]	局部中断攻击	识别名称前缀层次结构来检测异常	异常前缀	设置黑名单, 阻止恶意流量传输	按名称前缀限制	中	全网路由器
文献[60]	局部中断攻击	PIT 命中率、兴趣包请求速率等	异常接口	限制异常兴趣的传输	按内容限制	小	边缘路由器和 IC
文献[63]	虚假局部攻击	自适应神经模糊推理系统	异常兴趣	构造缓存替换策略	按节点控制是否缓存	大	全网路由器
文献[64]	虚假局部攻击	安装蜜罐监视用户	异常兴趣	将异常兴趣加入黑名单并显示通告上游	按异常兴趣	中	需额外基础设施

由以上分析可以看出, 无论是按接口还是节点限制都会对正常用户造成误伤, 影响正常内容的缓存性能。未来工作中, 完善策略的关键在于检测异常的流量、用户、网络接口, 等等, 随着神经网络技术的不断发展, 若将其应用于异常检测, 检测粒度将越来越小, 从而可以更大程度地预防 DoS 攻击。另外可以设计更好的缓存机制, 在提高缓存性能的同时实现缓存污染攻击的防御。

表 3 给出了几种典型缓存污染攻击检测和防御策略的对比。

5 CCN 中的拥塞控制技术研究

由于 CCN 网络传输与传统的 TCP/IP 网络传输不同, 所以传统的 TCP 拥塞控制算法和传输协议不能直接应用于 CCN 网络, 主要存在以下问题:

(1) 由于 CCN 中多源[66]的传输的新特性使得基于重传超时(Retransmission Timeout, RTO)的拥塞检测在 CCN 中不再可靠。基于 TCP 中单源连接(单条路径)的 RTO 检测机制在 CCN 中不再可靠, 因为来自不同源或不同路径的 RTT 是不同的。更重要的是,

由于数据包可能来自不同的源节点[67], 无序传送或到达时间间隔的变化不能指示网络状态。

(2) 基于重复 ACK 的拥塞检测不再适用。由于 CCN 数据包是独立命名的, 并且一个数据包响应一个兴趣包, 对于丢失的数据包, 接收端会重新发送相应的兴趣包, 并且发送方不会在收到相同的兴趣请求之前重复发送相同的数据[68]。也就是说, 它不需要有序的数据包传输, 接收端不能通过接收重复的 ACK 来检测丢失。因此, 传统 TCP 中基于重复 ACK 的隐式拥塞检测机制不再适用于 CCN。

(3) 基于单个拥塞控制窗口的速率控制机制在 CCN 中不再适用。TCP 的拥塞控制窗口(congestion window, cwnd)调整适用于单一路径的网络传输, 它通过不断调整其 cwnd 大小来适应单个路径的瓶颈带宽。然而, 由于 CCN 中的多源传输特性, 单个 cwnd 控制不能适应多源传输。例如, 假设一个内容请求者通过两条不同的路径接收来自两个源的数据, 如果一条路径拥塞并且内容请求者减少了它的 cwnd, 它也将减少另一条没有拥塞的路径的流量。

(4) 自时钟机制可能导致流行和不流行的内容之间的公平性问题。对于 TCP 的自动时钟, 数据发送速率取决于传入 ACK 的速率, 具有不同 RTT 的竞争 TCP 发送器将以不同的速率接收 ACK, 同样会以不同的速率增加其发送窗口。这一现象被称为 TCP 的 RTT-bias[69]。由经验得出, 在一定的吞吐量下, 竞争 TCP 流量与其 RTT 成反比。

另一方面, CCN 网络中的拥塞控制也有其自身的特点:

(1) 接收端的流量控制能力。因为它采用了请求驱动的“拉”式传输方式和一个兴趣包对应一个数据包的传输模式, 因此可以通过控制接收端的兴趣流量来控制数据流量。由于兴趣包的大小比数据包小得多, 拥塞主要由数据包流量引起, CCN 的数据传输方式可以直接控制拥塞, 而在 TCP/IP 网络中只能在发生拥塞后才能做出回应, 控制导致拥塞的数据流量。与 TCP/IP 网络相比, 这是 CCN 的一个优势。

(2)中间节点可用于拥塞控制。由于 CCN 使用一个兴趣包对应一个数据包的传输模式, 因此可以通过控制兴趣包的发送速率来控制数据包流量, 从而实现流量控制。另一方面, 通过调整兴趣包的发送速率, 可以防止由拥塞导致的数据包的丢失。因此, 在 CCN 中, 可以通过调节兴趣包的请求和转发速率来控制数据包的返回速率, 从而实现网内拥塞控制。

网络拥塞是指由于用户的请求过多使得网络中某些资源被耗尽, 导致路由器缓冲区溢出, 兴趣包或数据包被丢弃, 从而使得网络整体性能下降。由于 CCN 节点为每个向上游转发的兴趣包接收响应数据包, 然后在每个接口向下游发送, 如果接口处数据包的到达速率超过下行链路传输容量, 则数据包开始排队并且有些最终被丢弃, 导致数据包的超时和重传。每个兴趣包有一个特定的生命周期, 当生命周期到期但没有获得请求的内容时, 内容请求者需要重新发送兴趣包。另外, PIT 记录了尚未被满足的兴趣包, 因此 PIT 也是一个潜在的瓶颈, 限制了可向网络上游转移的兴趣包数量, 从而也限制了数据包的数量。因此, 在 CCN 中, 网络拥塞不仅可以从接收端进行控制, 还可以从中间节点进行控制, 现有的 CCN 拥塞控制机制从这两个角度出发进行设计, 根据拥塞控制的模式, 本文将这些机制分为三类: 基于接收端的控制方法、逐跳控制方法和混合方法。

5.1 基于接收端的控制方法

CCN 中最早的控制兴趣转发速率的方法之一是使用兴趣控制协议(Interest Control Protocol, ICP)[70], 它采用 TCP 中的 AIMD 窗口调整算法, 根据 RTO 定时器是否超时来检测拥塞, 设置 RTO 定时器 τ 的值的算法也与 TCP 相似。同时, 它为每个兴趣包设置 RTO 计时器, 并测量每个返回的数据包的 RTT, 当 RTO 超时被触发时, 拥塞控制窗口将被乘法减少。但是此协议没有考虑同时有多个数据源对数据进行响应的情况。

解决多源问题的一种传统解决方案是为每个内容源维护一个单独的 RTO 值。在 CCN 中, 每个内容对象被分成多个数据包大小的块。当传输内容对象时, 路径上的路由器可以缓存单个块, 这些块可用于为其他用户的后续请求提供服务。由于 CCN 中的内容块可以从多个不同节点的缓存中检索, 数据源在网络工作过程中可能频繁变化, 根据 RTT 估计设置适当的超时值是不可能的, 因此设置超时值的隐式反馈传输协议无法高效工作。

为了解决这个问题, 文献[71]提出了一种以内容为中心的传输控制协议(Content Centric TCP, CCTCP), 它考虑了来自多个来源的内容检索。CCTCP 为每个内容流维护多个拥塞窗口和 RTO 值, 由于接收端为每个内容流保留了多个 RTO 值, 因此需要一种机制来估计数据包来自哪里, 以便触发正确的 RTO。因此, 作者利用一种新颖的预期兴趣机制在请求内容块之前可靠地预测内容块的位置, 从而应对 RTT 不可预测性, 准确地估计重传超时。在请求者发出的每个兴趣包中, 都包含有后续预期请求的兴趣信息, 当中间路由器 k 接收到兴趣包时, 验证

自身是否存储接收端随后请求的任何数据块。如果路由器至少有一个预期兴趣的内容块, 则将自身缓存中存在的块的标识符、处理兴趣包时的时间戳 T_I 和唯一的节点标识符附加到该兴趣包, 路由器不得更改任何以前路由器附加的预期组块的可用性信息。如果路由器在其缓存中保存当前请求的内容块, 它将兴趣包中的包含预期分块的报头信息附加到数据包上, 并返回给请求者。在数据包的返回路径中, 每个路由器必须分析包含预期内容分块的报头信息, 如果报头包含附加到兴趣包的路由器的信息, 则路由器用当前时间 T_D(其处理数据包时)与 T_I 之间的差值替换绝对时间戳 T_I。此外, 路由器还会向数据包附加一个跳数, 该跳数最初设置为 0, 并且该路由计数将通过到达接收端的路径上的其他路由器递增, 接收端收到数据包后分析该跳数, 以了解路径上的缓存的拓扑顺序。同时, 使用包含在数据包报头中的信息, 接收节点可以根据公式(1)估计其自身与包含有预期兴趣内容块的路由器 k 之间的 RTT。

$$RTT(k) = (T_D - T_I) - (T_D(k) - T_I(k)) \quad (1)$$

T_I 和 T_D 分别由接收端发送兴趣包和接收到数据包时测量, $T_D(k)$–$T_I(k)$由路由器 k 测量, 并附加到返回的数据包上。CCTCP 可以有效地解决由于这种内容缓存分散导致的性能问题, 而不需要中间路由器中维护每个内容流状态。而且, 由于信息自身包含在预期的兴趣包报头中, 因此, 此机制不需要路由器维护任何用户状态。但是为每个内容流维护多个拥塞窗口和 RTO 值, 处理数据包时会耗费较多时间来解析包头部的信息。

解决多源问题的一个新思路是使用显式拥塞检测和通知方法, 其基本思想是接收端根据路由器反馈的显式拥塞信息调整自己的兴趣包发送速率, 中间路由器节点周期性地通过检测平均队列长度来检测其拥塞状态。如果拥塞发生, 拥塞路由器会将拥塞信息反馈给下游节点。现存的主要有两种显式通知方式, 一种是发送特殊的控制信号包 NACK[72]来通知网络拥塞, 另一种是通过使用特殊位字段使用数据包携带拥塞信息。标记的数据包或特殊的 NACK 包沿着数据转发路径向下游转发给接收端, 当经过中间节点时, 拥塞状态信息将通过比较原始拥塞等级和在该节点本身中检测到的等级来更新。一旦收到明确的拥塞信息, 接收端将相应地调整其兴趣包发送速率, 通过这种方式, 接收端不再需要隐含地估计网络拥塞状态。

(1) 使用特殊的控制信号包 NACK

中间节点可以通过显式发送拥塞控制数据包 NACK(negative acknowledgments)来协调通知请求者拥塞, 当 CCN 节点既不能满足也不能进一步转发兴趣包时, 它将信号包 NACK 发回到下游节点。如果下游节点已经耗尽了所有自己的转发选项, 它会向下游发送 NACK。信号包 NACK 携带与原始兴趣包相同的名称和随机数, 加上一个 NACK 代码, 解释为什么兴趣包不能被满足或转发, 以便相应采取适当的措施, 但是, 向下游发送 NACK 的缺点是这可能需要消息优先化并引起额外开销。

(2) 使用特殊位字段通过数据包携带拥塞信息

在定时器到期之前明确地向内容请求者通知网络拥塞是正确的, 但明确地向流量源发出拥塞信息不应该需要消息优先化或导致额外的网络开销。文献[73]提出的拥塞控制协议在数据包头中标记一个选项字段, 用此字段的标记数值来通知下游节点发生了网络拥塞。默认情况下, 将 CCN 数据包报头中的 1 位选项字段 OF 设置为 0, 当网络发生拥塞时, 将 OF 设置为 1。每个接收数据包的下游节点检查 1 位 OF, 以此来推断上游网络拥塞。如果 OF 是 1, 则节点可以在转发信息表中尝试其他可用的传出接口。这种通过传输路径多样化来应对网络拥塞的方法能够降低上游节点的负载, 通过给定接口在数据包头中标记一个可选字段, 可以避免任何额外的流量进入网络造成网络资源浪费。

当上游网络拥塞时, 数据块可能需要更长的时间才能返回, 从而导致 PIT 中每个 PIT 条目的持续时间增加, 并可能导致 PIT 阻塞。另外, 当 PIT 占用率增加时, 可能导致数据缓冲区工作量增加, 拥塞可能发生在数据缓冲区中。因此, 为使 CCN 拥塞控制机制有效, 必须考虑 PIT 的占用率, 并且 PIT 的当前占用率可用于估计缓冲区的未来占用率。在通信网络中, 最好的情况是在发生拥塞之前避免拥塞, 因此, 可以使用 PIT 占用率来估计下一个 RTT 中的数据包传输缓冲区的预期队列长度。Abu 等[73]提出一种机制, 利用 PIT 的占用情况作为在不久的将来在数据包队列中排队的附加数据的良好估计器, 该机制首先控制 PIT 的拥塞, 其次控制路由器的缓冲区的拥塞。作者基于 PIT 的拥塞控制机制考虑了 PIT 的占用情况并预测每个中间节点下一个 RTT 中的数据缓冲区的占用情况, 当预期的队列大小超过阈值时, 向请求者传递显式拥塞通知以减慢他们的兴趣包发送速率。当在 PIT 或路由器缓冲区中检测到拥塞时, CCN 接收节点会在重新传输计时器到期之前收到通知, 收到通知后就相应地调整发送速率。

5.2 逐跳控制方法

在 TCP/IP 网络中, 中间节点负责转发数据包, 拥塞控制主要是针对终端节点。但是, 在 CCN 网络中, 中间节点可以使用 PIT 来记录待定兴趣并可以控制兴趣包转发速率, 因此, 与 CCN 中的另一种拥塞控制模式是逐跳控制方法。

逐跳控制方法的基本原理如下: 每个 CCN 节点检测拥塞并调整兴趣包的转发速率, 以控制相应返回数据包的传输速率, 从而实现网络拥塞控制。通常, 中间节点通过检测到达的数据队列长度来检测它自己的拥塞状态, 如果拥塞, 它将降低转发兴趣包的速率。典型的逐跳兴趣包转发速率调整算法是 HoBHIS(Hop-By-Hop Interest Shaping)[74], 它通过监测内容块队列长度来检测拥塞, 并根据队列占用情况和可用资源调整兴趣包转发速率, 节点的速率调整过程如图 5 所示。

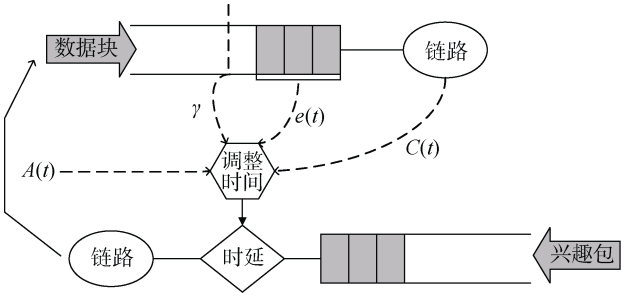

图 5 HoBHIS 节点速率调整模型

Figure 5 HoBHIS node rate adjustment model

当数据组块到达传输队列时, 路由器根据队列占用率 $e(t)$和可用资源(可用带宽 $C(t)$和一个响应延迟 $A(t)$(即一个 RTT)期间内的空闲队列长度)计算兴趣率 $\gamma(t)$, 如公式(2)所示。如果队列长度小于某个阈值 γ, 则路由器可以临时增加兴趣包发送速率, 否则, 路由器将降低其兴趣包发送速率。

$$\gamma(t) = C(t) + h\frac{r - e(t)}{A(t)} \tag{2}$$

Rozhnova 等[75]扩展了 HoBHIS 的设计, 提出了一种容错机制来控制内容请求者兴趣包发送速率并防止兴趣包丢失。除了对自身的兴趣包转发速率进行调整之外, 中间节点还利用 NACK 反馈和多路径转发机制向其下游节点通知拥塞状态, 并对接口性能进行标记和排序, 从而根据接口性能进行自适应多路径转发来缓解网络拥塞。

这种逐跳拥塞控制模式适用于 CCN 网络传输中无连接和多源的特点, 大多数现有的逐跳 CCN 拥塞控制算法简单地假设带宽是已知并且恒定的, 因此路由器使用其接口带宽作为两个 CCN 节点之间的可用链路带宽来调整兴趣包转发速率。但是这些假设是不符合实际的, 可能不适用于覆盖链路、无线链路或应用程序。为了解决这个问题, Shi 等[76]提出了一种实用的拥塞控制机制(Practical Congestion control scheme, PCON), PCON 路由器通过使用从 CoDel[77]扩展的主动队列管理(Active Queue Management, AQM)方案来检测其本地链路上的拥塞。每个节点通过监视其传出队列来检测本地拥塞(通过在 CCN 链路抽象之上实现一个填充层[78]来可靠地指示给定分组是否在某个“链路”上丢失), 当检测到拥塞时, 路由器通过使用数据包特殊位字段标记方法向用户和下游路由器和内容请求者发送拥塞状态信号, 下游路由器通过将后续兴趣包部分地转移到备选路径, 内容请求者调整兴趣包发送速率来防止网络继续拥塞。同时, 在无线和覆盖网络链路上, 一旦检测到拥塞, 该方案使用 NACK 发回拥塞信号。可以看出, PCON 虽然也是逐跳控制机制, 但是与传统逐跳控制机制有本质区别: PCON 路由器不是像传统策略一样根据对传入兴趣包对应的数据包将占用多少链路容量的预测而丢弃兴趣包, 而是在传出链路上监视队列, 这可以提前发出拥塞信号并隐含地考虑可用带宽。

5.3 混合方法

纯粹的基于接收端的控制方法在拥塞检测中可能不完全准确, 且如果只在终端实施速率控制机制, 可能存在公平性问题, 而中间节点的控制可以调节所有流量(例如, 它可以根据每个流量的公平比率来调节流量)。另一方面, 纯粹的逐跳控制机制不足以保证最佳的传输性能, 因为终端的最优初始发送速率不是先验值, 而是在不断变化的可用网络资源[36], 因此, 有些研究人员将两种机制结合起来形成一种混合机制来更好的控制网络拥塞。

Carofiglio 等[79]提出了一个名为 HR-ICP(Hop-by-hop and Receiver-Driven Interest Control Protocol)的混合方法, 该方法是使用 ICP 机制的同时增加了逐跳拥塞机制。在接收端, 该方法使用 ICP 兴趣包控制算法(如 5.1 节所述), 并在中间节点使用以下算法: 在每个输出接口中, HR-ICP 为每个流维护一个虚拟队列, 并与一个信用计数器关联起来, 信用计数器表示该流被允许传输的数据字节数并初始化为最大值, 该计数器的值根据下行链路估计的公平率的增长而增加, 根据转发兴趣数量的增加而减少。流代表单个内容检索, 当至少有一个兴趣包在输出缓冲区中排队或者信用计数器为空时, 定义该流为瓶颈流,

虚拟队列的生命周期与 PIT 中的相关兴趣包的生命周期相同。当一个兴趣包到达一个接口时, 该节点检查它是否属于瓶颈流。如果该内容流不是瓶颈流, 则兴趣包将直接被转发出去, 并且信用计数器减少相应数据包的字节数; 若该内容流属于瓶颈流, 兴趣包将在向下传递的流量队列中排队以进行速率适配。值得注意的是, 在 HR-ICP 中, 基于接收端的机制和逐跳控制机制是相互独立的, 二者之间没有协作。

Ndikumana 等[80]基于接收端的控制机制和逐跳控制机制相互协作, 提出了一种新的基于内容中心网络的合作和全分布拥塞控制机制(Novel Cooperative and Fully-distributed Congestion Control Mechanism for Content Centric Networking, NCFCC)。NCFCC 将基于本地测量的合作和存储效率令牌桶机制 (Cooperative and Memory-efficient Token Bucket, CMTB)与全分布拥塞控制机制(Fully- Distributed Congestion Control, FDCC)组合成一个混合拥塞控制机制, 其中 FDCC(在内容请求者节点处)防止拥塞并根据 CMTB(在中间节点)生成的降低发送速率(reduce sending rate, RSR)消息调整流量速率。CMTB 控制数据包在中间节点中注入网络的速率, 而 FDCC 根据接收到的内容块和拥塞信息控制内容请求者节点中的流量速率。RSR 用作 CMTB 和 FDCC 算法之间的链路, 用于交换相邻节点之间的拥塞信息, 帮助内容请求者节点在无需等待兴趣包到期或超时的情况下调整兴趣包发送速率, 还可以帮助中间节点根据队列长度调整每个链路的流量速率。通过监视缓冲区利用率, NCFCC 能够在发生拥塞之前防止拥塞, 该方案不是在发生拥塞状态时进行测量, 而是通过监控缓冲区利用率并调整流量率来防止拥塞。

以上所述的方案中, 抵御拥塞的解决方案之一是通知内容请求者使其降低兴趣包发送速率, 但是, 消费者降低兴趣包发送速率影响所有链路分支上的流量, 这意味着即使对于非拥塞路径, 兴趣包转发速率也受到监管和控制, 这对于正常路径是不公平的。为了解决公平性问题, Miyoshi 等[81]提出了一种新的接收端的机制和逐跳控制机制协作的拥塞控制方法, 该方法由端到端窗口流控制和路由器兴趣转发控制两部分组成, 实现了仅在拥塞的链路分支上调节传输速率。首先路由器检测到拥塞后向兴趣包来时的反向路径上发送 NACK 通知拥塞, 当路由器从一个链路分支收到 NACK 后, 计算该分支的窗口缩减率, 并将计算结果通过 NACK 分组传送给内容请求者, 同时根据窗口缩减率成比例地减少该 NACK 到达接口转发兴趣包的概率。内容请求者通过 AIMD 策略控制其拥塞窗口大小, 当 NACK 分组到达时, 窗口大小与由该 NAK 分组携带的窗口缩减率成比例地减小。

文献[81]所提方案通过控制拥塞分支路由器与内容请求者的兴趣包转发速率实现仅调节拥塞分支上的兴趣包传输速率, 避免了其他非拥塞分支受到影响, 解决了公平性问题。另外, PCON 能够适应无线链路的可用带宽变化, 这解决了当前兴趣包发送速率调整算法依赖恒定带宽的问题。但是, CCN 拥塞控制方案中的准确性和成本问题, 对内容请求者收到拥塞消息后无响应该如何有效处理的问题等等都是未来工作需要解决的问题。另外, 用人工智能方法可以提前预测网络拥塞, 而不是等网络拥塞之后再通知下游链路控制流量, 进而增强网络的可用性。

由以上方案的总结分析可以看出, 现有 CCN 拥塞控制方案的不足在于不能很好的预测将要到来的拥塞, 未来可以设计更好的自适应转发策略, 根据网络资源分配动态调整要转发的内容, 如使用强化学习中的 Q-Learning 算法[82]实现自适应路由转发策略, 实现智能化的路由, 让路由策略自己“学会”选择最优路径。

6 展望与总结

6.1 未来研究展望

本文主要围绕 CCN 安全技术的最新研究成果进行综述, 介绍了近年来在隐私保护、DoS 攻击和拥塞控制方面代表性的解决方案。但是, CCN 中的安全技术还是一个新兴的研究领域, 现有解决方案仍然存在一些不足之处, 很多具有挑战性的问题有待进一步解决:

1) CCN 网络安全态势感知与预测

网络安全态势感知与预测能够使网络安全人员宏观把握网络的安全状态, 为管理人员提供决策支持, 能够提高网络安全事件的应对与防范能力。当前, 针对 CCN 安全的研究主要集中在隐私保护、DoS 攻击防御、拥塞控制等单项技术方面, 难以对 CCN 的安全状态进行准确评估。另外, 由于 CCN 与 TCP/IP 网络存在本质区别, 现有面向 TCP/IP 的网络安全态势感知与预测技术难以直接应用到 CCN 中。因此, 需要针对 CCN 网络特点, 构建面向 CCN 的网络安全态势评估体系与模型, 并在此基础上研究安全态势感知算法与预测算法。

针对上述问题, 首先基于 CCN 网络的分布式特点, 设计分布式数据采集系统获取能够引起 CCN 网络安全态势发生变化的安全要素参数; 其次, 基于大数据理论与系统对采集到的多源数据进行处理、分析, 得出过去与当前的网络安全态势, 并预测安全态势的发展趋势; 最后, 基于预测结果采用人工智能技术选择合适的应对与防御策略。

2) 面向特定应用场景的 CCN 安全技术研究

CCN 作为未来网络领域中一种极具发展潜力的网络架构, 具有内容分发效率高、内容获取时延小等优点, 且能客服 IP 网络中地址空间耗尽、移动性支持差等问题。因此, 已有研究人员将 CCN 应用到物联网(Internet of Things, IoT)[83]、车联网(Internet of Vehicles, IoV)[84]等应用场景, 并证明了 CCN 的有效性。但是, 对于这些场景下 CCN 的安全技术研究较少, 而且不同应用场景的安全需求不尽相同, 因此需要对特定应用场景的 CCN 安全技术进行研究。

针对上述问题, 首先需要分析各种应用场景的特点, 例如物联网场景下的 CCN 节点具有类型多样、性能较弱等特点, 车联网场景下的 CCN 业务具有时延小、可靠性高等特点; 其次, 针对不同应用场景设计不同的安全架构与协议, 例如对于物联网场景需要设计普适性高、轻量级的安全架构与协议, 对于车联网场景需要设计低时延高可靠的安全架构与协议。

3) CCN 网络内容监管

CCN 是一种以内容核心、以提高内容分发效率为目标的分布式网络, 网络节点可以直接基于内容名称进行通信, 且在通信过程中不包含节点身份信息。由于 CCN 具有无中心性, 在提高网络中内容分发效率的同时, 也为不良信息的传播、散布提供了温床。因此, 需要有效地实施对 CCN 的内容安全监管, 控制不良或非法信息的传播, 进而营造健康的网络环境。

针对上述问题, 首先, 将内容监管领域中的概念、关系、属性等进行明确化、形式化和规范化的描述, 凝练出领域知识, 形成以敏感人群、网络行为、信息内容等概念为中心的监管本体和知识库, 建立内容监管知识模型; 其次, 基于“用户、行为、内容”的敏感数据感知平台, 对 CCN 中信息数据集进行初步筛选, 降低冗余信息量; 最后, 建立动态感知网络, 对可疑潜在的内容、用户进行实时跟踪分析, 对相关事件关联分析及阻断取证, 做到快速发现、及时阻止。

6.2 未来工作

随着 CCN 技术的发展, 特别是 CCN 被纳入 5G 标准之后, CCN 中的安全技术已经成为未来网络领域的研究热点。目前, 研究者主要针对 CCN 中的隐私保护、DoS 攻击、拥塞控制等三个方面做了很多工作。本文对内容中心网络中的安全问题进行了总结和分析, 介绍了隐私泄露、DoS 攻击和网络拥塞三个主要安全问题, 分析了网络中的安全需求, 回顾和总结了最近几年国内外在上述三个问题上的主要研究成果, 并对这些安全问题的解决方案进行对比分析, 进而分别针对各个安全问题提出潜在的对策, 最后提出了 CCN 中仍然存在的安全问题和未来的研究方向。归纳来讲, CCN 的安全技术仍是国内外的一个研究热点, 但已有研究成果仍存在不足, 所以仍然有大量关键的问题还需要进一步深入细致地研究。

参考文献

[1] Cisco Visual Networking Index: Forecast and Methodology, 2015–2020. Accessed: Aug. 15, 2017. [Online]. Available: http://www.communicationstoday.co.in/reports/8556-ciscovisual-networking-indexforecast-and-methodology-2015-2020.

[2] V. Jacobson, J. Burke, L. Zhang, et al. Named data networking (NDN) project 2013- 2014 report, http://named-data.net, Annual Progress Report, 2014.

[3] Pan J L, Paul S, Jain R. A Survey of the Research on Future Internet Architectures[J]. *IEEE Communications Magazine*, 2011, 49(7): 26-36.

[4] Koponen T, Chawla M, Chun B G, et al. A Data-oriented (and beyond) Network Architecture[J]. *ACM SIGCOMM Computer Communication Review*, 2007, 37(4): 181.

[5] Jacobson V, Smetters D K, Thornton J D, et al. Networking Named Content[C]. *the 5th international conference on Emerging networking experiments and technologies*, 2009: 1-12.

[6] NDN. http://named-data.net/.

[7] S. Tarkoma, M. Ain, K. Visala. The publish/subscribe internetrouting paradigm (psirp): Designing the future internet architecture[C]. In*Future Internet Assembly*, 2009: 102–111.

[8] PSIRP. http://www.psirp.org/.

[9] B. Ahlgren, M. D’Ambrosio, M. Marchisio, et al. Design considerations for a network of information[C]. *the ACM CoNEXT Conference*, 2008: 1-66.

[10] Seskar I, Nagaraja K, Nelson S, et al. MobilityFirst Future Internet Architecture Project[C]. *the 7th Asian Internet Engineering Conference*, 2011: 1-3.

[11] Gasti P, Tsudik G, Uzun E, et al. DoS and DDoS in Named-Data

Networking[EB/OL]. 2012: arXiv:1208.0952[cs.NI]. https://arxiv.org/abs/1208.0952.

[12] Afanasyev A, Mahadevan P, Moiseenko I, et al. Interest Flooding Attack and Countermeasures in Named Data Networking[C]. *CST*. 2013:1-9.

[13] Karami A. Data Clustering for Anomaly Detection in Content-Centric Networks[J]. *International Journal of Computer Applications*, 2013, 81(7): 1-4.

[14] Li Y, Xin Y H, Han Y N, et al. A Survey of DoS Attack in Content Centric Networking[J]. *Journal of Cyber Security*, 2017, 2(1): 91-108.
(李杨, 辛永辉, 韩言妮, 等. 内容中心网络中 DoS 攻击问题综述[J]. 信息安全学报, 2017, 2(1): 91-108.)

[15] Afanasyev A, Mahadevan P, Moiseenko I, et al. Interest Flooding Attack and Countermeasures in Named Data Networking[C]. *CCN*. 2013:1-9.

[16] Tang H B, Zheng L H, Ge G D, et al. Detection Algorithm for Cache Pollution Attacks Based on Node State Model in Content Centric Networking[J]. *Journal on Communications*, 2016, 37(9): 1-9.
(汤红波, 郑林浩, 葛国栋, 等. CCN 中基于节点状态模型的缓存污染攻击检测算法[J]. *通信学报*, 2016, 37(9): 1-9.)

[17] Y. Gao. Internet cache pollution attacks and countermeasures[C]. *IEEE ICNP*, 2006: 865-861.

[18] Andersson L, Davies E, Zhang L. Report from the IAB Workshop on Unwanted Traffic March 9-10, 2006[R]. RFC Editor, 2007.

[19] C. Yi, A. Afanasyev, I. Moiseenko, et al. A case for stateful forwarding plane[J]. *Comput. Commun.*, 2013, 36(7): 779–791.

[20] Tourani R, Misra S, Mick T, et al. Security, Privacy, and Access Control in Information-Centric Networking: A Survey[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(1): 566-600.

[21] Chaabane A, de Cristofaro E, Kaafar M A, et al. Privacy in Content-oriented Networking[J]. *ACM SIGCOMM Computer Communication Review*, 2013, 43(3): 25-33.

[22] Chaabane A, de Cristofaro E, Kaafar M A, et al. Privacy in Content-oriented Networking[J]. *ACM SIGCOMM Computer Communication Review*, 2013, 43(3): 25-33.

[23] Misra S, Tourani R, Majd N E. Secure Content Delivery in Information-centric Networks: Design, Implementation, and Analyses[C]. *the 3rd ACM SIGCOMM workshop on Information-centric networking*, 2013: 73-78.

[24] C A. Wood, E. Uzun. Flexible end-to-end content security in CCN[C]. *Consumer Communications and NETWORKING Conference. IEEE,* 2014:858-865.

[25] M R. Asghar, C. Bernardini, B. Crispo. PROTECTOR: Privacy-preserving information lookup in content-centric networks[C]. *IEEE International Conference on Communications. IEEE,* 2016:1-7.

[26] G. Acs, M. Conti, P. Gasti, et al. Cache privacy in named-data networking[C]. *IEEE 33rd Int. Conf. Distrib. Comput.Syst. (ICDCS)*, 2013: 41–51.

[27] Chaabane A, de Cristofaro E, Kaafar M A, et al. Privacy in Content-Oriented Networking: Threats and Countermeasures[EB/OL]. 2012: arXiv:1211.5183[cs.CR]. https://arxiv.org/abs/1211.5183.

[28] Mohaisen A, Mekky H, Zhang X W, et al. Timing Attacks on Access Privacy in Information Centric Networks and Countermeasures[J]. *IEEE Transactions on Dependable and Secure Computing*, 2015, 12(6): 675-687.

[29] Zhu Y, Mi Z K, Wang W N. Cache Pollution Defense Technologies in Content Centric Networking[J]. *Journal of Nanjing University of Posts and Telecommunications*, 2015, 35(2): 27-33.
(朱轶, 糜正琨, 王文甭. 内容中心网络缓存污染防御技术研究[J]. *南京邮电大学学报(自然科学版)*, 2015, 35(2): 27-33.)

[30] Ge Guodong, Guo Yunfei, Liu Caixia, et al. A Collaborative Caching Strategy for Privacy Protection in Content Centric Networking[J]. *Journal of Electronics & Information Technology*, 2015, 37(5): 1220-1226.
(葛国栋, 郭云飞, 刘彩霞, 等. 内容中心网络中面向隐私保护的协作缓存策略[J]. *电子与信息学报*, 2015, 37(5): 1220-1226.)

[31] Wu Q H, Li Z Y, Tyson G, et al. Privacy-Aware Multipath Video Caching for Content-Centric Networks[J]. *IEEE Journal on Selected Areas in Communications*, 2016, 34(8): 2219-2230.

[32] C. Wood, M. Mosko, E. Uzun. CCNx Key Exchange Protocol Version 1.0[C]. *Internet-Draft draft-wood-icnrg-ccnxkeyexchange- 00, Internet Engineering Task Force*, 2014:125-130.

[33] E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3[C]. Internet-Draft draft-ietf-tls-tls13-14, *Internet Engineering Task Force*, 2016: 158-161.

[34] Liu Y, Bai X F, Yang Y B. Privacy Protection Strategy in Content-centric Networking Based on Multi-layer Encryption Mechanism[J]. *Computer Engineering and Applications*, 2017, 53(5): 1-5.
(柳毅, 白雪峰, 杨育斌. 基于多层加密机制的内容中心网络隐私保护策略[J]. *计算机工程与应用*, 2017, 53(5): 1-5.)

[35] Liao H J, Richard Lin C H, Lin Y C, et al. Intrusion Detection System: A Comprehensive Review[J]. *Journal of Network and Computer Applications*, 2013, 36(1): 16-24.

[36] S Signorello, S Marchal, J Francois, et al. Advanced interest flooding attacks in named-data networking[C]. *IEEE, International Symposium on Network Computing and Applications. IEEE Computer Society,* 2017:1-10.

[37] H Dai, Y Wang, J Fan, et al. Mitigate DDoS attacks in NDN by interest traceback[C]. *Computer Communications Workshops. IEEE*, 2014:381-386.

[38] A Compagno, M Conti, P Gasti, et al. Poseidon: Mitigating interest

flooding DDoS attacks in Named Data Networking[C]. *Local Computer Networks. IEEE,* 2013:630-638.

[39] Afanasyev A, Mahadevan P, Moiseenko I, et al. Interest Flooding Attack and Countermeasures in Named Data Networking[C]. 2013:1-9.

[40] Floyd S, Jacobson V. Link-sharing and Resource Management Models for Packet Networks[J]. *ACM Transactions on Networking*, 1995, 3(4): 365-386.

[41] Karami A. Data Clustering for Anomaly Detection in Content-Centric Networks[J]. *International Journal of Computer Applications*, 2013, 81(7): 1-4.

[42] Li X L, Jia C, Liu D X, et al. Nonlinear Adaptive Control Using Multiple Models and Dynamic Neural Networks[J]. *Neurocomputing*, 2014, 136: 190-200.

[43] Gan M, Peng H, Dong X P. A Hybrid Algorithm to Optimize RBF Network Architecture and Parameters for Nonlinear Time Series Prediction[J]. *Applied Mathematical Modelling*, 2012, 36(7): 2911-2919.

[44] Zhang Z Y, Wang T, Liu X G. Melt Index Prediction by Aggregated RBF Neural Networks Trained with Chaotic Theory[J]. *Neurocomputing*, 2014, 131: 368-376.

[45] Karami A, Guerrero-Zapata M. A Hybrid Multiobjective RBF-PSO Method for Mitigating DoS Attacks in Named Data Networking[J]. *Neurocomputing*, 2015, 151: 1262-1282.

[46] Deb K, Pratap A, Agarwal S, et al. A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II[J]. *IEEE Transactions on Evolutionary Computation*, 2002, 6(2): 182-197.

[47] Davies D L, Bouldin D W. A Cluster Separation Measure[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1979, PAMI-1(2): 224-227.

[48] Montazer G A, Khoshniat H, Fathi V. Improvement of RBF Neural Networks Using Fuzzy-OSD Algorithm in an Online Radar Pulse Classification System[J]. *Applied Soft Computing*, 2013, 13(9): 3831-3838.

[49] Park C M, Rehman R A, Kim B S. Packet Flooding Mitigation in CCN-Based Wireless Multimedia Sensor Networks for Smart Cities[J]. *IEEE Access*, 2017, 5: 11054-11062.

[50] Amadeo M, Molinaro A, Ruggeri G. E-CHANET: Routing, Forwarding and Transport in Information-Centric Multihop Wireless Networks[J]. *Computer Communications*, 2013, 36(7): 792-803.

[51] Hyun S, Kim H. Secure and DoS-Resilient Fragment Authentication in CCN-Based Vehicular Networks[J]. *Wireless Communications and Mobile Computing*, 2018, 2018: 1-12.

[52] H. Salah, J. Wulfheide, T. Strufe. Coordination supports security: A new defence mechanism against interest flooding in NDN[C]. *IEEELCN*, 2015: 268-270.

[53] H. Salah, T. Strufe. Evaluating and mitigating a collusive versionof the interest flooding attack in ndn[C]. *IEEE ISCC*, 2016:124-130.

[54] Perino D, Varvello M. A Reality Check for Content Centric Networking[C]. *the ACM SIGCOMM workshop on Information-centric networking*, 2011: 127-130.

[55] H. Park, I. Widjaja, H. Lee. Detection of cache pollution attacksusing randomness checks. *IEEE International Conference on Communications (ICC)*, 2012: 1096–1100.

[56] M Xie, I Widjaja, H Wang. Enhancing cache robustness for content-centric networking[C]. *IEEE INFOCOM*, 2012:2426-2434.

[57] Xylomenos G, Ververidis C N, Siris V A, et al. A Survey of Information-Centric Networking Research[J]. *IEEE Communications Surveys & Tutorials*, 2014, 16(2): 1024-1049.

[58] Conti M, Gasti P, Teoli M. A Lightweight Mechanism for Detection of Cache Pollution Attacks in Named Data Networking[J]. *Computer Networks*, 2013, 57(16): 3178-3191.

[59] T. Kamimoto. Cache protection method based on prefix hierarchy for content-oriented network[C]. *IEEE CCNC,* 2016:125-130.

[60] H Salah, M Alfatafta, S Sayedahmed, et al. CoMon++: Preventing Cache Pollution in NDN Efficiently and Effectively[C]. *IEEE, Conference on Local Computer Networks. IEEE,* 2017:43-51.

[61] J Gouge, ASeetharam, S Roy. On the scalability and effectiveness of a cache pollution based DoS attack in information centric networks[C]. *International Conference on Computing, NETWORKING and Communications. IEEE*, 2016:1-5.

[62] A. Karimipoor. Effectiveness of cache pollution attacks in ICN cache services[C]. *Diss.* 2017: 136-137.

[63] Karami A, Guerrero-Zapata M. An ANFIS-based Cache Replacement Method for Mitigating Cache Pollution Attacks in Named Data Networking[J]. *Computer Networks*, 2015, 80: 51-65.

[64] G. Mauri, R. Raspadori, M. Gerlay, et al. Exploiting information centric networking to build an attacker-controlled contentdelivery network[C]. In *Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET),* 2015:1-6.

[65] G. Marfia, C. Palazzi. TCP Libra: Exploring RTT-Fairness for TCP[C]. *NETWORKING,* 2007: 1005–1013.

[66] Mick T, Tourani R, Misra S. MuNCC: Multi-hop Neighborhood Collaborative Caching in Information Centric Networks[C]. *the 2016 conference on 3rd ACM Conference on Information-Centric Networking*, 2016: 93-101.

[67] G. Carofiglio, M. Gallo, L. Muscariello,et al. Multipath congestion control in content-centric networks[C]. *IEEE INFOCOM 2013 Workshop onEmerging Design Choices in Name-Oriented Networking*, 2013: 268-270.

[68] L. Saino, C. Cocora, G. Pavlou. CCTCP: a scalable receiver-driven congestion control protocol for content centric networking[C]. *IEEE ICC'13*, 2013: 268-270.

[69] L. Zhang, D. Estrin, J. Burke, et al. Nameddata networking (NDN)

project[C]. *NSF Project Proposal*, 2010:268-270.

[70] G. Carofiglio, M. Gallo, L. Muscariello. ICP: design and evaluation of an interest control protocol for content-centric networking[C]. *IEEE INFOCOMWorkshop on Emerging Design Choices In Name Oriented Networking (INFOCOM NOMEN),* 2012: 285-290.

[71] L Saino, C Cocora, G Pavlou. CCTCP: A scalable receiver-driven congestion control protocol for content centric networking[C]. *IEEE International Conference on Communications. IEEE,* 2013: 3775-3780.

[72] Yi C, Afanasyev A, Moiseenko I, et al. A Case for Stateful Forwarding Plane[J]. *Computer Communications*, 2013, 36(7): 779-791.

[73] A J Abu, B Bensaou, A M Abdelmoniem. Inferring and Controlling Congestion in CCN via the Pending Interest Table Occupancy[C]. *LCN*, 2016: 433-441.

[74] N. Rozhnova, S. Fdida. An extended hop-by-hop Interest shaping mechanism for content-centric networking[C]. *IEEE GLOBECOM*, 2014:25-30.

[75] N Rozhnova. Congestion control for Content-Centric Networking[J]. *IEEE Transactions on Industrial Informatics*, 2017, 14(6):272-275.

[76] S Shi, Y Ren, Li, et al. A content store-based congestion control algorithm for named data networking[J]. *Chinese High Technology Letters*, 2016, 23(2):258-260.

[77] Nichols K, Jacobson V. Controlled Delay Active Queue Management[R]. RFC Editor, 2018.

[78] S. Vusirikala, S. Mastorakis, A. Afanasyev, et al. A best effort link layer reliability scheme. Technical report[R], *NDNTR41*, 2016.

[79] Carofiglio G, Gallo M, Muscariello L. Joint Hop-by-hop and Receiver-driven Interest Control Protocol for Content-centric Networks[C]. the second edition of the ICN workshop on Information-centric networking, 2012: 23-28.

[80] Ndikumana A, Ullah S, Thar K, et al. Novel Cooperative and Fully-Distributed Congestion Control Mechanism for Content Centric Networking[J]. *IEEE Access*, 2017, 5: 27691-27706.

[81] Miyoshi J, Kawauchi S, Bandai M, et al. Multi-Source Congestion Control for Content Centric Networks[C]. *the 2016 conference on 3rd ACM Conference on Information-Centric Networking*, 2016: 205-206.

[82] F Farahnakian, M Ebrahimi, M Daneshtalab, et al. Q-learning based congestion-aware routing algorithm for on-chip network[C]. *IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications. IEEE*, 2012: 258-260.

[83] Lei K, Zhong S R, Zhu F X, et al. An NDN IoT Content Distribution Model with Network Coding Enhanced Forwarding Strategy for 5G[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(6): 2725-2735.

[84] Chowdhury M, Gawande A, Wang L. Secure Information Sharing among Autonomous Vehicles in NDN[C]. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 2017: 236-240.

朱大立 于 2007 年 12 月在华中科技大学计算机应用技术专业获得博士学位。现任中国科学院信息工程研究所第四研究室正高级工程师。研究领域为移动互联网安全。研究兴趣包括安全智能终端, 无线网络空口协议安全。Email: zhudali@iie.ac.cn

李婷 于 2018 年在重庆大学通信工程专业获得学士学位。现于中国科学院信息工程研究所攻读硕士学位。研究领域为 5G、未来网络。研究兴趣为移动边缘计算和内容中心网络。Email: liting0715@iie.ac.cn.

耿立茹 于 2018 年在北京邮电大学信息与通信工程专业获得硕士学位。现任中国科学院信息工程研究所研究实习员。研究领域为: 移动通信与安全。研究兴趣包括: 5G 网络安全、移动通信业务管控等。Email: gengliru@iie.ac.cn

梁杰 于 2016 年在青岛大学网络工程专业获得学士学位。现在中国科学院信息工程研究所攻读硕士学位。研究领域为未来网络中的缓存优化技术研究。研究兴趣包括: 内容中心网络、缓存优化、内容流行度预测。Email: liangjie@iie.ac.cn

张杭生 于 2017 年在浙江工业大学数字媒体技术专业获得工学学士学位, 现在中国科学院大学网络空间安全专业攻读硕士学位。研究领域为大数据安全, 社交网络热度预测与信息溯源, 网络安全溯源分析, 研究兴趣包括信息传播规律的研究, 大规模图数据存储与分析。Email: zhanghangsheng@iie.ac.cn

吴荻 于 2014 年在北京交通大学通信与信息系统专业获得博士学位。现任中科院信息工程研究所助理研究员。研究领域为移动网络、传感网等。研究兴趣包括: 物联网、隐私保护、无线资源分配等。Email: wudi@iie.ac.cn

张天魁 于2008年在北京邮电大学通信与信息系统专业获得博士学位。现任北京邮电大学信息与通信学院副教授。研究领域为: 未来网络理论、移动通信。研究兴趣包括: 信息中心网络、移动蜂窝边缘缓存技术、无线资源分配等。
Email: zhangtiankui@bupt.edu.cn

刘银龙 于 2011 年在北京邮电大学通信与信息系统专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为: 未来网络理论、移动通信与安全。研究兴趣包括: 信息中心网络理论与应用、移动通信业务管控等。
Email: liuyinlong@iie.ac.cn